POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 2022

ALCALDÍA DE GUADALAJARA DE BUGA

APROBADO POR:
COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO

Versión 3.0

Alcalde Julián Adolfo Rojas Monsalve
Guadalajara de Buga

TABLA DE CONTENIDO

INTRODUCCIÓN

La Alcaldía Municipal de Guadalajara de Buga establece su Política de Administración del Riesgo con los parámetros necesarios para identificar, analizar la causa raíz, valorar, gestionar, monitorear y revisar aquellos eventos negativos que puedan afectar o impedir el logro de sus objetivos institucionales. Para tal evento se han identificado dos clases de riesgos: de Gestión y de Corrupción.

La Alta Dirección lidera el proceso de Administración de Riesgos de la entidad acorde con la legislación vigente aplicable y la Guía para la Administración del Riesgo – Versión 5 de diciembre 2020, del Departamento Administrativo de la Función Pública - DAFP. Los líderes estratégicos (Alta dirección, Secretarios y Jefes de Oficina), líderes de procesos y participantes en dichos procesos, son los responsables de la identificación, análisis y valoración de riesgos de gestión y de corrupción, la definición de acciones de control para éstos y la actuación correctiva y oportuna ante la materialización de los riesgos identificados.

Todos los servidores públicos de la entidad son responsables de la reducción de los riesgos y de velar por la eficacia de los controles integrados en los procesos, actividades y tareas a su cargo.

La Oficina de Control Interno, es responsable de evaluar en forma independiente el componente Administración de Riesgos, como parte integral del Sistema de Control Interno y el cumplimiento y efectividad de las políticas de riesgos.

1. OBJETIVO

Definir los parámetros necesarios para lograr identificar, analizar, valorar, mitigar, aplicar y evidenciar los controles de los riesgos de gestión y de corrupción, con el fin minimizar los efectos adversos y desviaciones al interior de la Entidad y evitar el incumplimiento de los objetivos institucionales.

2. ALCANCE

La Política de Administración del Riesgo inicia desde la definición de los parámetros necesarios para identificar, analizar y valorar los riesgos de gestión y de corrupción hasta la determinación de los niveles de aceptación, el tratamiento y el seguimiento de los mismos.

3. ÁMBITO DE APLICACIÓN

La Política de Administración del Riesgo es aplicable a todos los programas, proyectos, planes y/o procesos de la Entidad, así como también a las acciones ejecutadas por los servidores públicos durante el ejercicio de sus funciones.

4. TÉRMINOS Y DEFINICIONES

Riesgo de Gestión: Posibilidad de efecto que se causa sobre el cumplimiento de los objetivos de las entidades debido a eventos potenciales.

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 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/IEC27000).

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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 las cuales se puede presentar el riesgo.

Impacto: Las consecuencias que puede ocasionar a la organización la materialización del 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.

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 debe o desea gestionar.

Riesgo Residual: Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Control: Medida que permite reducir o mitigar un riesgo.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Integridad: Propiedad de exactitud y completitud.

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

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

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

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la Entidad.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección que no sería posible el logro de los objetivos de la Entidad.

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.

Apetito de 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 de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

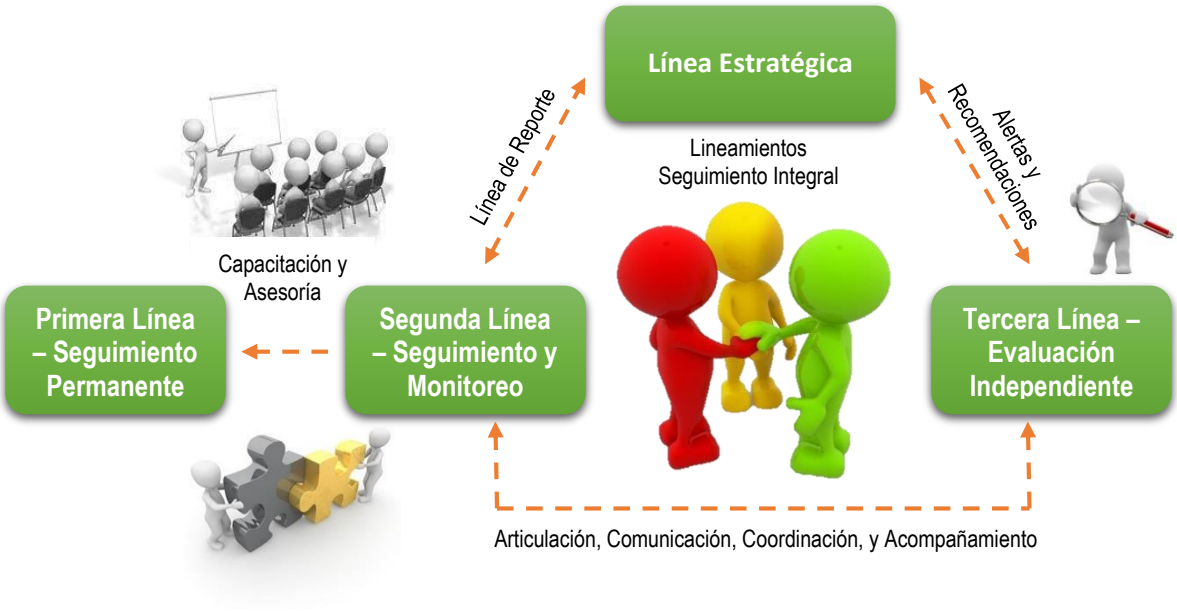
Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo es Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la
Multiplicación, por ejemplo, mediante una Matriz de Probabilidad – Impacto.

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.

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.

Fuente: Dirección de Gestión y Desempeño Institucional de la Función Pública; Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 5; P. 12

5. RESPONSABLES Y LINEAS DE DEFENSA



Fuente: Adaptado de la Guía de Administración del Riesgo Versión No.5 del 2020 por la Coordinación de Calidad

La Función Pública dentro del marco del Modelo Integrado de Planeación y Gestión MIPG, desarrolla en la Dimensión 7 (Control Interno) las Líneas de Defensa, en las cuales se definen las responsabilidades de la Gestión del Riesgo y Controles, de modo que cada grupo de Servidores Públicos de la Administración Municipal de Guadalajara de Buga entienda el alcance de sus responsabilidades y cómo se articula su rol en la estructura general del Riesgo y Control de la Organización.

A continuación se detalla las responsabilidades de las líneas de defensa frente a la Administración del Riesgo y Controles de la Alcaldía de Guadalajara de Buga:

LINEA DE DEFENSA	PROPÓSITO	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
LINEA ESTRATÉGICA	Esta línea al ser una instancia decisoria dentro del sistema de Control Interno, está bajo la responsabilidad de la Alta Dirección y del Comité Institucional de Coordinación de Control Interno; su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (Política de Administración del Riesgo) y el cumplimiento de los planes en la entidad.	Alta Dirección y Comité Institucional de Coordinación de Control Interno	✓Emitir, revisar, validar y supervisar la Política de Administración del Riesgo y garantizar el cumplimiento de la misma. Hacer seguimientos a la gestión y al Plan Anual de auditoría interna en la entidad. ✓Fortalecimiento del Comité Institucional de Coordinación de Control Interno, incrementando su periodicidad para las reuniones. ✓Evaluación de la forma como funciona el esquema de Líneas de Defensa, incluyendo la Línea Estratégica. ✓Lineamientos para el seguimiento, análisis de los controles de los riesgos de Gestión y Corrupción y establecimiento de acciones de mejora por parte de los Secretarios y Jefes de Oficina. ✓Hacer seguimiento a los niveles de aceptación del riesgo con el fin de determinar posibles cambios que favorezcan el cumplimiento de los objetivos de la Entidad. ✓Revisar y analizar los cambios en el entorno (contexto interno y externo) para identificar posibles impactos que generen modificaciones en la definición de riesgos y controles de la entidad.

			✓Analizar el informe de evaluación a la gestión de riesgos y realizar propuestas de mejora para el tratamiento de los mismos. ✓Evaluar el estado del Sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.
PRIMERA LÍNEA DE DEFENSA	Esta línea está bajo la responsabilidad, principalmente, de los líderes de programas, procesos y proyectos (Secretarios de Despacho, Asesores y Jefes de Oficina) y de sus equipos de trabajo, en general servidores públicos en todos los niveles de la organización; su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol".	Líderes de Proceso, Secretarios de Despacho, Jefes de Oficina y equipos de trabajo, en general servidores públicos en todos los niveles de la organización	✓Conocimiento y apropiación de las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo. ✓Identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. ✓Seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda. ✓Formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. ✓Coordinación con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa.

SEGUNDA LÍNEA DE DEFENSA	Esta línea está bajo la responsabilidad, principalmente, del Jefe de Planeación o quienes haga sus veces, coordinadores de equipos de trabajo, comité de contratación, áreas financieras y de TIC, entre otros, que respondan de manera directa por el aseguramiento de la operación; su rol principal es asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces; así mismo, consolidan y analizan la información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos, todo lo anterior enmarcado en la "Autogestión".	Secretaría de Planeación	✓Aseguramiento de que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces. ✓Consolidación y análisis de información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. ✓Trabajo coordinado con las oficinas de control interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno. ✓Asesoría 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. ✓Establecimiento de los mecanismos para la autoevaluación requerida (auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora).

TERCERA LÍNEA DE DEFENSA	Esta línea está bajo la responsabilidad de los Jefes de control interno o quienes hagan sus veces; desarrollaran su labor a través de los siguientes roles a saber: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento.	Oficina de Control Interno	✓Enfoque a la Prevención: Articula la Asesoría y Acompañamiento con el fomento de la Cultura del Control. ✓A través de su Rol de Asesoría, Orientación Técnica y recomendaciones frente a la Administración del Riesgo en Coordinación con la Oficina Asesora de Planeación para garantizar el cumplimiento efectivo de los objetivos. ✓Monitoreo a la exposición de la Organización al Riesgo y realizar recomendaciones con alcance preventivo. ✓Asesoría proactiva y estratégica a la Alta Dirección y los Líderes de Proceso, en materia de Control Interno y sobre las responsabilidades en materia de Riesgos. ✓Formar a la Alta Dirección y a todos los niveles de la Entidad sobre las responsabilidades en materia de Riesgos. ✓Revisar, Analizar y Recomendar mejoras a la Política de Administración del Riesgo.

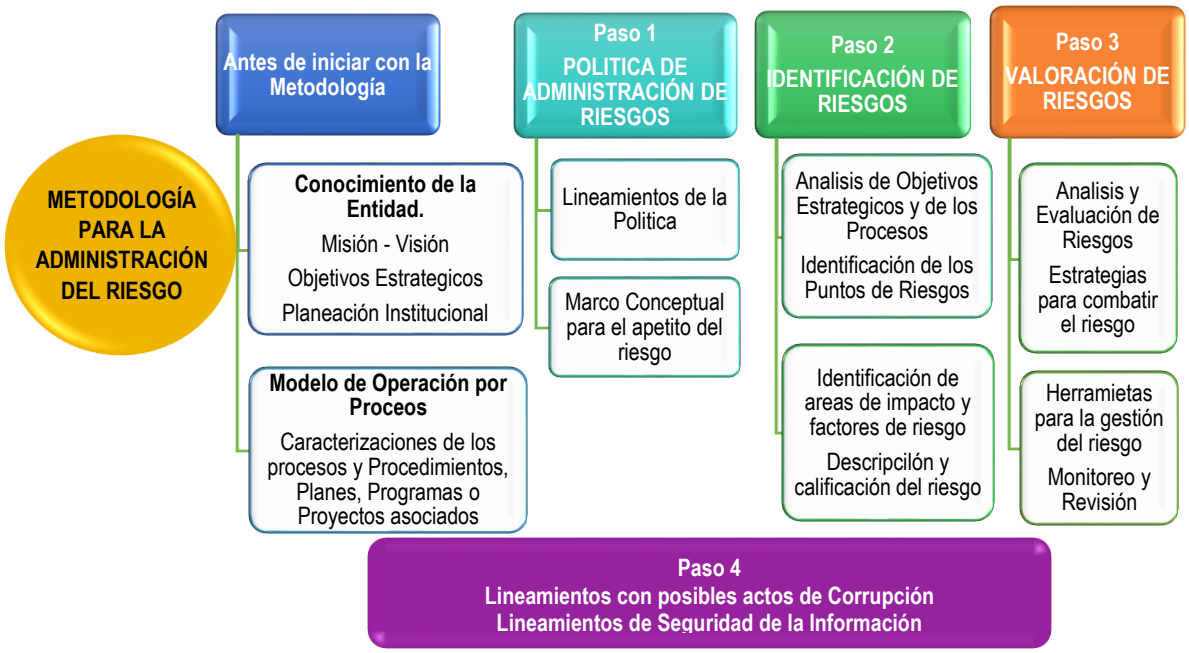
Fuente: Las responsabilidades para la Administración del Riesgo y Controles de la Alcaldía municipal de Guadalajara de Buga se definieron con base en la Implementación de las líneas de defensa descritas en el Manual Operativo del Modelo Integrado de Planeación y Gestión, Versión 4, de Marzo de 2021, Pagina 116..

6. CONTEXTO GENERAL DE LA ENTIDAD PARA LA ADMINSITRACIÓN DEL RIESGO

Antes de iniciar con la metodología para administrar los riesgos es necesario comprender el contexto general de la Alcaldía de Guadalajara de Buga (Factores internos y externos), ya que el conocimiento del contexto facilita la identificación de riesgos y oportunidades para el cumplimiento de los objetivos estratégicos de la Entidad.

Este contexto se compone del **Contexto Interno** (Misión, Visión, Estructura Organizacional, Funciones y Responsabilidades, Políticas, Planeación Institucional, Objetivos y Estrategias Implementadas, Recursos con los que se cuenta (Económicos, Personas, Procesos, Sistemas, Tecnología, Información), Cultura Organizacional y Relaciones con las partes involucradas), **Contexto Externo** (Factores: Políticos, Económicos, Financieros, Sociales, Culturales, Tecnológicos, Ambientales, Legales y Reglamentarios), y **Contexto del Proceso** (Objetivo y Alcance del proceso, Interrelación con otros procesos, planes, programas o proyectos asociados y activos de seguridad digital del proceso). El análisis del contexto general de la Entidad permite reconocer en dónde se encuentra la organización al revisar y establecer su direccionamiento y objetivos.

7. METODOLOGÍA GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO



8. NIVELES DE ACEPTACIÓN DEL RIESGO

La Alcaldía Municipal de Guadalajara de Buga determina que para los riesgos residuales de gestión y seguridad digital que se encuentren en Zona de Riesgo baja, está dispuesto a Aceptar el riesgo y no se requiere la documentación de Planes de Acción, sin embargo, se deben monitorear conforme a la periodicidad establecida. Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
Riesgos de Gestión y Riesgos de Seguridad de la Información	Baja	Se **ACEPTA** el riesgo y se administra mediante revisiones trimestrales para determinar el estado del riesgo.
	Moderado	Se determina **REDUCIR (Mitigar o Compartir)** el riesgo mediante acciones de control que permitan mitigar la probabilidad de ocurrencia o impacto del riesgo. Se realiza seguimiento trimestral por parte del Secretario o Jefe de Oficina para analizar el comportamiento del riesgo.
	Alto y Extremo	Se debe dar prioridad a estos riesgos y establecer monitoreo periódico por parte del líder del proceso, con el objetivo de evitar la materialización del mismo. Se determina **REDUCIR (Mitigar o Compartir)** el riesgo mediante acciones de control que permitan mitigar la probabilidad de ocurrencia o impacto del riesgo. Se realiza seguimiento trimestral por parte del Secretario o Jefe de Oficina para analizar el comportamiento del riesgo.
Riesgos de Corrupción	Baja	Ningún riesgo de corrupción podrá ser aceptado. Periodicidad mensual de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.
	Moderado	Se establecen acciones de control preventivas que permitan **REDUCIR (Mitigar o Compartir)** la probabilidad de ocurrencia del riesgo. Periodicidad mensual de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra en el Tablero de Riesgos y Controles
	Alto y Extremo	Se adoptan medidas para: **REDUCIR (Mitigar o Compartir)** 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.

9. METODOLOGÍA PARA LA IDENTIFICACIÓN, ANÁLISIS, VALORACIÓN Y TRATAMIENTO DEL RIESGO

9.1 Herramientas para la Administración del Riesgo

Para la identificación, análisis, valoración y tratamiento de los Riesgos de Gestión y de Corrupción se deben utilizar los formatos SIG.CT-01-F3 “Matriz de Riesgos de Gestión 2022” y SIG.CT-01-F4 “Matriz de Riesgos de Corrupción 2022”, en los cual se define el Impacto, las causas inmediatas y causa raíz de los riesgos identificados, la valoración del riesgo inherente, las acciones de control, el responsable de seguimiento, la valoración del riesgo residual (después de haber aplicado el control) y el análisis de seguimiento respectivo de cada riesgo por parte de Secretarios o Jefes de Oficina, por cada proceso asociado de los Macroprocesos de la Alcaldía Municipal de Guadalajara de Buga.

9.2 Clasificación de los Riesgos

A continuación las siguientes categorías permiten agrupar los riesgos identificados de la entidad.

TIPO DE RIESGO	CLASIFICACIÓN	DESCRIPCIÓN
RIESGOS DE GESTIÓN	EJECUCIÓN Y ADMINISTRACIÓN DE PROCESOS	Pérdidas derivadas de errores en la ejecución y administración de procesos.
	FALLAS TECNOLÓGICAS	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
	RELACIONES LABORALES	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
	USUARIOS, PRODUCTOS Y PRÁCTICAS	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

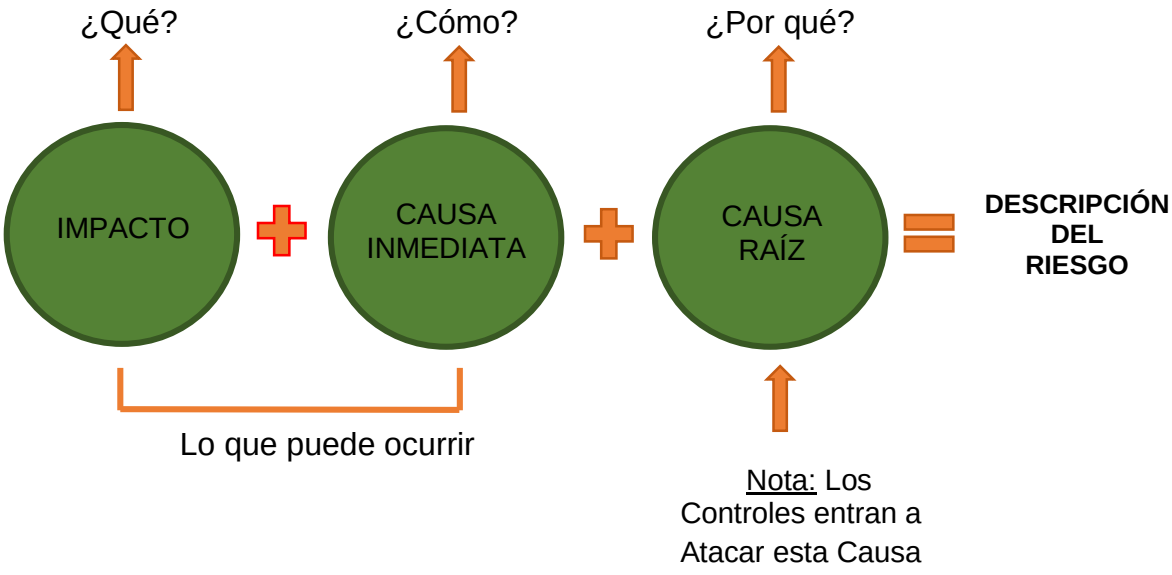
	DAÑOS A ACTIVOS FIJOS/ EVENTOS EXTERNOS	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
	LEGALES	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la entidad debido a su incumplimiento o desacato a la normativa vigente.
RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	PÉRDIDA DE CONFIDENCIALIDAD	Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital.
	PÉRDIDA DE INTEGRIDAD	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.
	PÉRDIDA DE DISPONIBILIDAD DE LOS ACTIVOS DE INFORMACIÓN	
RIESGOS DE FRAUDE	FRAUDE EXTERNO	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
	FRAUDE INTERNO	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales están involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
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.

Fuente: Adaptado de la Dirección de Gestión y Desempeño Institucional de la Función Pública; Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 5; P. 12

9.3 Metodología para la Administración de Riesgos de Gestión

9.3.1 Estructura para la Redacción del Riesgo de Gestión

Se adopta la estructura propuesta por la Dirección de Gestión y Desempeño Institucional de la Función Pública en la Guía de la Administración del Riesgo, Versión 5, para la descripción del riesgo el cual debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. La estructura facilita su redacción y claridad que inicia con la frase **POSIBILIDAD DE** y se analizan los siguientes aspectos:



La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

9.3.2 Criterios para definir la Probabilidad Inherente del Riesgo de Gestión

Se adopta la tabla No.4 de la Guía de la Administración del Riesgo, en su Versión 5 para determinar el nivel de probabilidad del Riesgo de Gestión, propuesto por la Función Pública, donde indica que la exposición al riesgo estará asociada al proceso

o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

A continuación se muestran los Criterios para determinar el nivel de Probabilidad del Riesgo de Gestión:

	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 25 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 501 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%

9.3.3 Criterios para definir el Nivel de Impacto Inherente del Riesgo de Gestión

Para la definición de los criterios de impacto, la Función Pública, en su Guía de la Administración del Riesgo, versión 5 agrupa los impactos en las variables de Afectación Económica y Reputacional; teniendo en cuenta que “cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferente niveles, se debe tomar el nivel más alto”. Bajo este esquema se adopta los criterios para definir el nivel de impacto del riesgo de gestión propuesta, puesto que facilita el análisis para el líder del proceso, dado que permite tener información objetiva para su establecimiento, y elimina la subjetividad en este tipo de análisis.

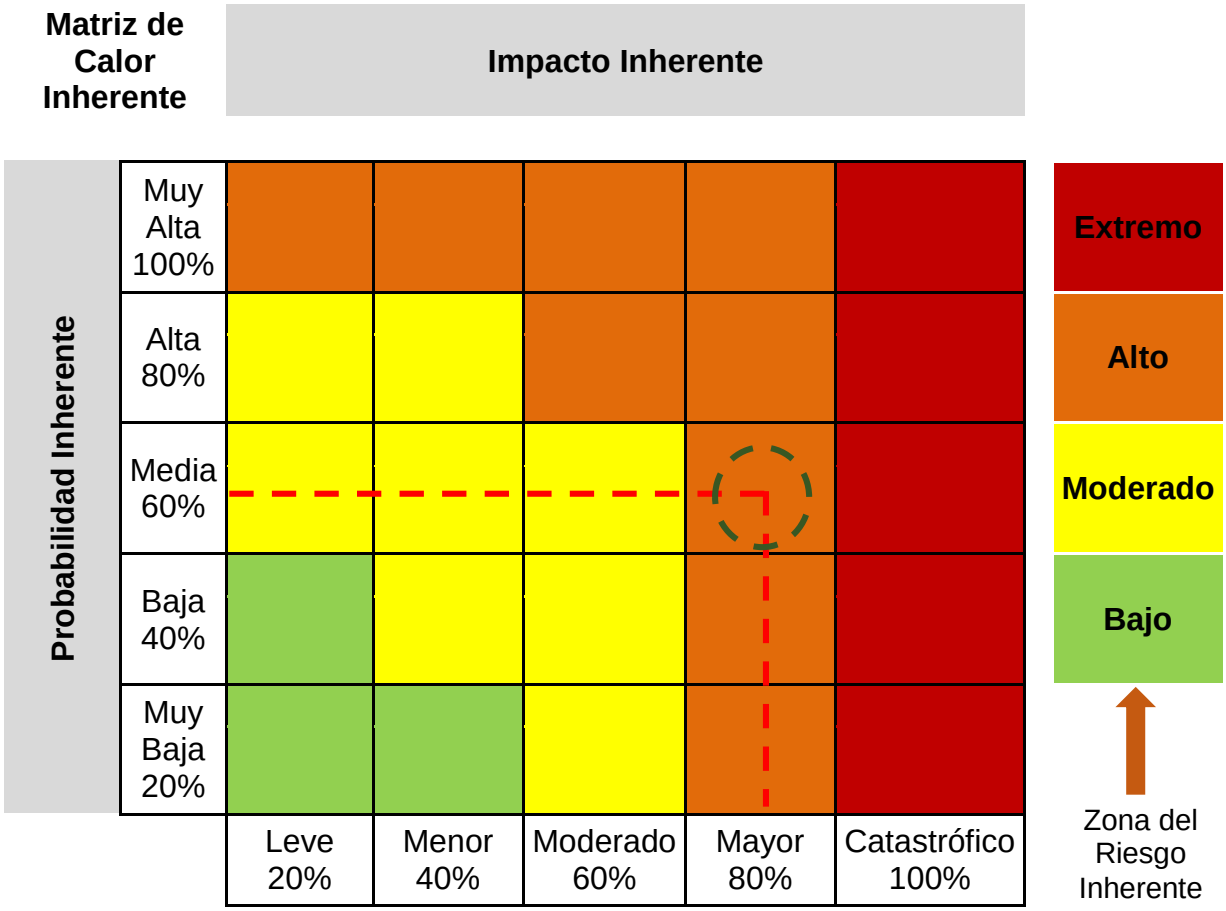
A continuación se muestran los Criterios para determinar el nivel de Probabilidad del Riesgo de Gestión:

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización
Menor 40%	Afectación desde 10 y hasta 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%	Afectación mayor a 50 y hasta 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Afectación mayor a 100 y hasta 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%	Afectación mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país

9.3.4 Matriz de Calor para la Evaluación del Riesgo de Gestión Inherente

Se adopta la matriz de calor para la evaluación del riesgo propuesta en la Guía de la Administración del Riesgo, versión 5, de la Función Pública, para establecer la Zona del Riesgo de Gestión Inherente (antes de aplicar Controles), a partir del análisis en el cruce de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, lo que permite determinar los niveles de severidad en los que puede estar expuesto el Riesgo identificado.

A continuación se muestra un ejemplo del cruce en la Matriz de Calor para la Evaluación del Riesgo de Gestión y se muestra los diferentes niveles de severidad adaptados en la Zona del Riesgo inherente:



9.3.5 Determinación y Valoración de Controles

La identificación y determinación de los controles se realiza a cada riesgo por los líderes de procesos o servidores expertos en su quehacer, de igual forma son los responsables de implementar y monitorear dichos controles con el apoyo de su equipo de trabajo. Dichos controles entran a atacar la **Causa Raíz** de cada riesgo identificado. El propósito de la implementación de controles, es comparar los resultados del análisis de riesgo inherente (sin controles) con los controles establecidos, para determinar la zona de riesgo final o "riesgo residual".

9.3.5.1 Estructura para la Descripción del Control

Para una adecuada redacción del control se adopta la estructura propuesta por la Función Pública en la Guía de la Administración del Riesgo, Versión 5, que facilita entender su tipología y otros atributos más adelante expuestos para su valoración.

La estructura es la siguiente:

Responsable de Ejecutar el Control + Acción + Complemento

- ✓ **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.

9.3.5.2 Análisis y Evaluación del Control

Para el análisis y evaluación de los controles se adopta la tipología y atributos propuestos por la Función Pública, los cuales permiten tener un diseño del control claro, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Cabe anotar que los aspectos de Tipo e Implementación, son atributos que tienen incidencia directa en la efectividad del control:

Características			Descripción	Peso
Atributos de Eficiencia	**Tipo**	**Preventivo**	Va hacia las causas del riesgo, aseguran el resultado final esperado.	**25%**
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	**15%**
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	**10%**

Atributos de Eficiencia	**Implementación**	**Automático**	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	**25%**
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	**15%**

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad:

Características			Descripción	Peso
Atributos informativos	**Documentación**	**Documentado**	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	**-**
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	**-**
	Frecuencia	**Continua**	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	**-**

Atributos informativos		**Aleatoria**	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.	**-**
	Evidencia	**Con registro**	El control deja un registro permite evidencia la ejecución del control.	**-**
		Sin registro	El control no deja registro de la ejecución del control.	**-**

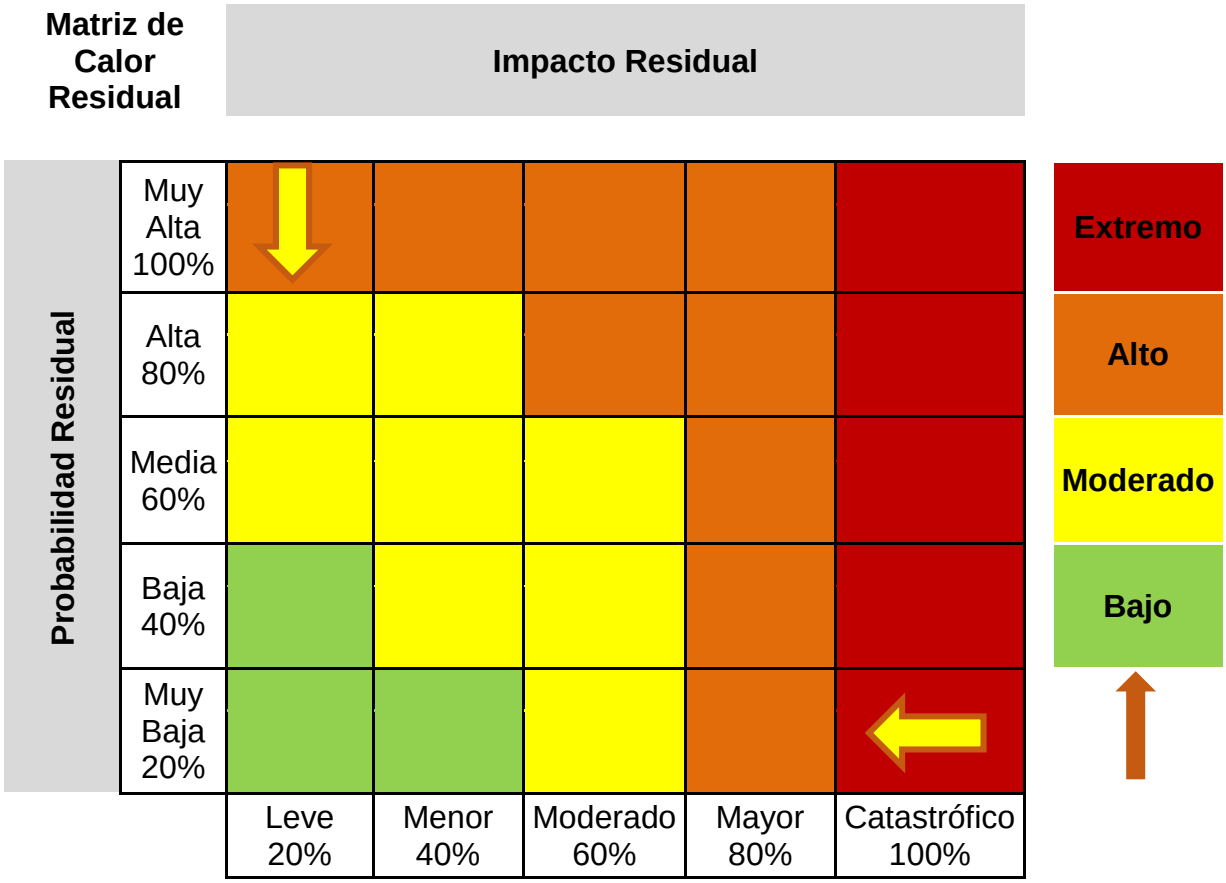
Fuente: Adaptado de la Guía de Administración del Riesgo Versión No.5 del 2020 por la Coordinación de Calidad

9.3.6 Valoración del Riesgo de Gestión Residual

A partir de los controles y la calificación de sus atributos, se dará movimiento del Riesgo en la Matriz de Calor Residual adaptada de la Guía de la Administración del Riesgo, Versión 5, Teniendo en cuenta que los controles de tipo Preventivo o Detectivo tienen afectación en la Probabilidad y los controles de tipo Correctivo afectan el Impacto.

CONTROLES PREVENTIVOS Y DETECTIVOS	CONTROLES CORRECTIVOS
⇩	⇩
ATACAN LA PROBABILIDAD	ATACAN EL IMPACTO

Estos movimientos se verán reflejados en la Matriz de Calor Residual que se muestra a continuación:



9.3.7 Estrategias de Tratamiento al Riesgo de Gestión y Plan de Acción

Cuando la Zona de Riesgo Residual o severidad se encuentra en un nivel bajo el Líder del proceso puede tomar la decisión de aceptar el riesgo y no debe de realizar plan de acción porque está dentro del nivel de aceptación del riesgo por la Alcaldía Municipal de Buga. Esto no aplica para los Riesgos de Corrupción.

Para las Zonas de Riesgo Residual o severidad que se encuentren en niveles Moderado, Alto o Extremo, el líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio de la implementación de los controles y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles. Después de haber implementado la acción se debe realizar un seguimiento por parte del Secretario de la dependencia o Jefe de Oficina con el fin de evaluar la efectividad del plan de acción en los tiempos establecidos en el Mapa de Riesgos.

9.4 Metodología para la Administración de Riesgos de Corrupción

9.4.1 Estructura para la Redacción del Riesgo de Corrupción

Se continúa con la estructura propuesta por la Dirección de Gestión y Desempeño Institucional de la Función Pública en la Guía de la Administración del Riesgo, Versión 4, puesto que en su versión 5 de Diciembre 2020, no hubo modificaciones para la identificación, análisis y valoración en los Riesgos de Corrupción.

A continuación se detalla la estructura de componentes que deben concurrir para la identificación y descripción de los Riesgos de Corrupción:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO

Cabe anotar que el riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos, y para facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se adopta la matriz de definición de riesgo de corrupción propuesta por la Dirección de Gestión y Desempeño Institucional de la Función Pública en la Guía de la Administración del Riesgo, Versión 4, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

MATRIZ: IDENTIFICACIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del Riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo Público	Beneficio privado
Ejemplo: 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

9.4.2 Criterios para definir la Probabilidad del Riesgo de Corrupción

Se adopta la tabla de la Guía de la Administración del Riesgo, en su Versión 4 del 2018 para determinar el nivel de probabilidad del Riesgo de Corrupción, propuesto por la Función Pública. Los criterios para definir el nivel de probabilidad son los siguientes:

Tabla Criterios para definir el nivel de probabilidad

Nivel		Descripción	Frecuencia de la Actividad	Probabilidad
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.	20%
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.	40%
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.	60%
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.	80%
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.	100%

9.4.3 Criterios para definir el Nivel de Impacto Inherente del Riesgo de Corrupción

Para la definición de los criterios de impacto, la Alcaldía de Guadalajara de Buga adopta la encuesta propuesta por la Función Pública, en su Guía de la Administración del Riesgo, versión 4 que se le realizará a cada líder del proceso para definir el impacto en caso de que se materialice el riesgo de corrupción. Al diligenciar la encuesta se establecerá una calificación entre los niveles: Moderado, Mayor y Catastrófico; Dicha calificación dependerá del número de respuestas afirmativas.

A continuación se muestran los Criterios para determinar el nivel de Impacto del Riesgo de Corrupción:

	ALCALDÍA MUNICIPAL DE GUADALAJARA DE BUGA	
	SISTEMA INTEGRADO DE GESTIÓN	SIG.CT-01-F2
		Rev. No. 1
	CRITERIOS PARA CALIFICAR EL IMPACTO (RIESGOS DE CORRUPCIÓN)	Fecha de Emisión: Noviembre 2021
		Página 1 de 1

MACROPROCESO:	
Proceso:	
Nombre del Riesgo:	

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?		

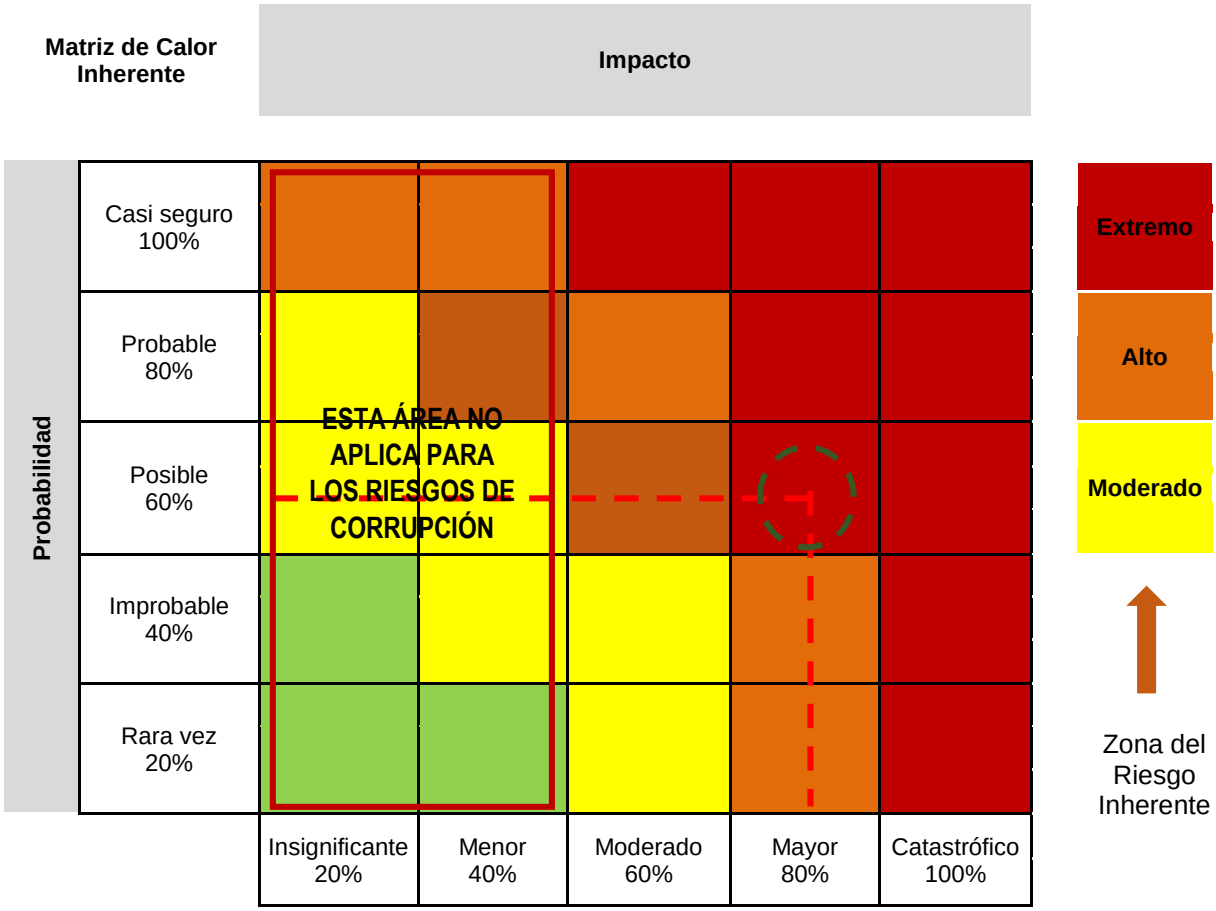
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la 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?		
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.		0	0

IMPACTO	**MODERADO:**	Genera medianas consecuencias sobre la entidad
	MAYOR:	Genera altas consecuencias sobre la entidad.
	CATASTRÓFICO:	Genera consecuencias desastrosas para la entidad

9.4.4 Matriz de Calor para la Evaluación del Riesgo de Corrupción Inherente

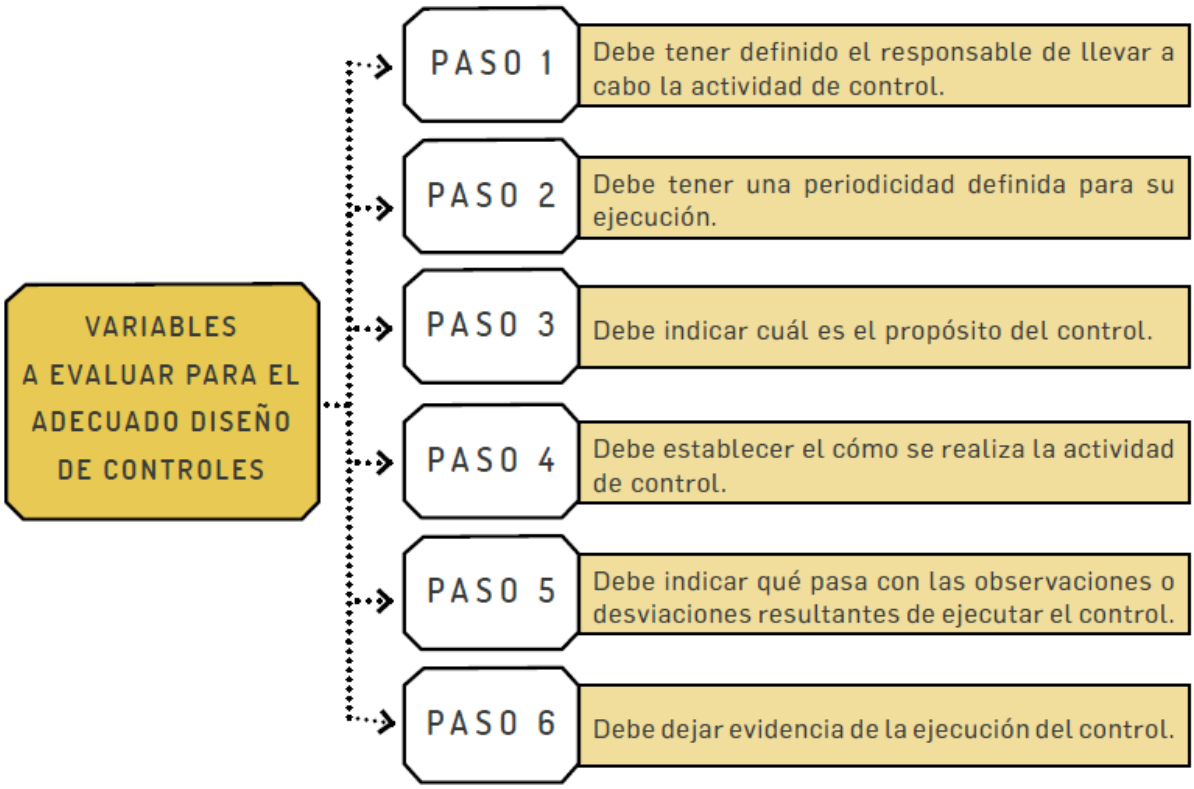
Se adopta la matriz de calor para la evaluación del Riesgo de Corrupción propuesta en la Guía de la Administración del Riesgo, versión 4, de la Función Pública, para establecer la Zona del Riesgo de Corrupción Inherente (antes de aplicar Controles), a partir del análisis en el cruce de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, lo que permite determinar los niveles de severidad en los que puede estar expuesto el Riesgo identificado.

A continuación se muestra un ejemplo del cruce en la Matriz de Calor para la Evaluación del Riesgo de Corrupción y se muestra los diferentes niveles de severidad adaptados en la Zona del Riesgo inherente:



9.4.5 Diseño de los Controles para Riesgos de Corrupción

Para una adecuada redacción del control se adopta la estructura propuesta por la Función Pública en la Guía de la Administración del Riesgo, Versión 5, mencionada anteriormente. Posteriormente se adoptan los 6 pasos para su diseño propuestos en la Versión 4 de la Función Pública:

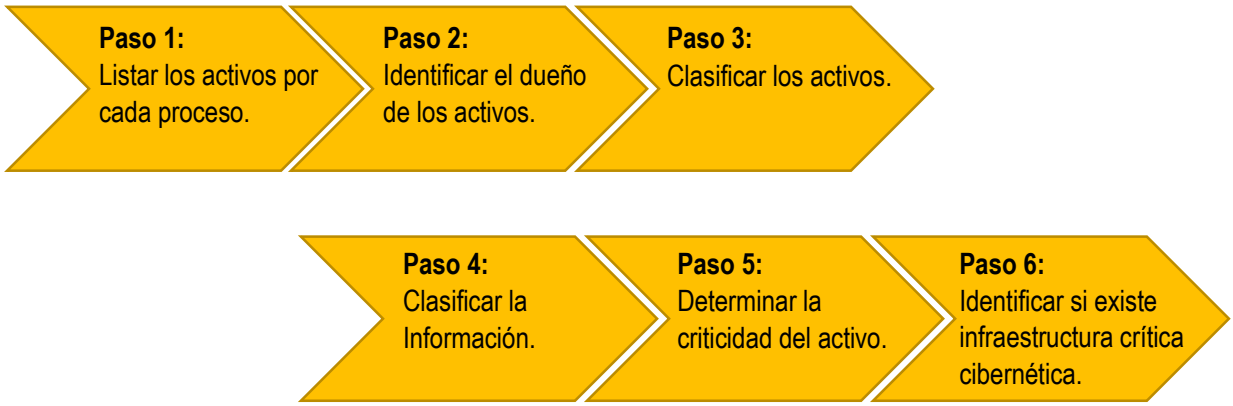


9.4.6 Estrategias de Tratamiento al Riesgo de Corrupción y Plan de Acción

Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento, el líder del proceso define acciones que permita mitigar el riesgo. Asimismo, determina la fecha de inicio de la implementación de los controles y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles a la Oficina de Control Interno. Después de haber implementado la acción se debe realizar un seguimiento por parte del Secretario de la dependencia o Jefe de Oficina con el fin de evaluar la efectividad del plan de acción en los tiempos establecidos en el Mapa de Riesgos.

9.5 Metodología para la Administración de Riesgos de Seguridad de la Información

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del Proceso, por lo cual se adopta la metodología propuesta por la Dirección de Gestión y Desempeño Institucional de la Función Pública en la Guía de la Administración del Riesgo, Versión 5:



9.5.1 Identificación del Riesgo de Seguridad de la Información

Para la identificación de Riesgos de Seguridad de la Información se adoptan los lineamientos propuestos en la Guía para la Administración del Riesgo, Versión de Diciembre 2020, donde se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización, teniendo en cuenta que para la agrupación de activos debe ser el mismo tipo. Como también tener en cuenta de acuerdo a los lineamientos propuestos en la Guía para la Administración del Riesgo, Versión de Diciembre 2020, que la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control. Para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda

explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Nota: Se adopta la propuesta para realizar la identificación de activos donde se deberá remitir a la sección 3.1.6 del anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas” que hace parte de los anexos de Guía para la Administración del Riesgo, Versión 5 de Diciembre 2020

9.5.2 Criterios para definir el Nivel de Probabilidad e Impacto de los Riesgos de Seguridad de la Información

La determinación de la Probabilidad e Impacto de los Riesgos de la Seguridad de la Información se deben llevar a cabo de acuerdo con lo establecido en el aparte 9.3.2 “Criterios para definir el nivel de Probabilidad de Riesgos de Gestión” y el aparte 9.3.3 “Criterios para definir el Nivel el Impacto de Riesgos de Gestión” de la presente Política.

9.5.3 Determinación, Valoración de Controles y Tratamiento de los Riesgos de Seguridad de la Información

Los procesos podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles que se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas” que se encuentra en los anexos de la Guía para la Administración del Riesgo. Versión 5 de Diciembre 2020, siempre y cuando se ajusten al análisis de riesgos. Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

10. INDICADORES CLAVES DE RIESGO

Para realizar el monitoreo del cumplimiento (eficacia) e impacto (efectividad) de las actividades de los controles establecidos se adoptan los indicadores claves de riesgos propuestos en las Guías de la Administración del Riesgo en sus versiones 4 y 5 de las Función Pública donde para evaluar el cumplimiento de las actividades se adopta el siguiente indicador por cada riesgo:

Índice de cumplimiento de las actividades de control = # de actividades cumplidas / # de actividades programadas) x 100

También para llevar una colección de datos de datos históricos, por periodos de tiempo, se adoptan los siguientes indicadores como ejemplo:

Proceso: Secretaría TIC

Indicador: Tiempo de interrupción de aplicativos críticos en el mes

Métrica: Número de horas de interrupción de aplicativos críticos al mes

Esto permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

11. GESTIÓN DE EVENTOS HISTÓRICOS

Se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, y las fuentes de información como por ejemplo: PQRDS, Auditorías Internas o de Entes de Control, Informes por la 1ra o 2da Línea de Defensa, etc.

12. PROCEDIMIENTOS A REALIZAR SI SE MATERIALIZA EL RIESGO

En caso de que se llegue a materializar un Riesgo de Gestión, Riesgo de Seguridad de la Información o Riesgo de corrupción, en la siguiente tabla se establece el paso a paso a seguir para efectuar el plan de contingencia establecido.

TIPO DE RIESGO	RESPONSABLE	ACCIÓN
Riesgo de Corrupción	Líder de 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 - efecto 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 a la Secretaría de Planeación y a Control Interno sobre el hallazgo y las acciones tomadas.
	Oficina de Control Interno	1. Informar al líder del proceso y al Secretario o Jefe de Oficina sobre la desviación encontrada. 2. Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso y ajustar el mapa de riesgos. 3. Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver la desviación. 4. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.
Riesgos de Gestión y Riesgos de Seguridad de la Información (Zona	Líder de 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 efecto, y determinar acciones correctivas y de mejora,

Extrema, Alta y Moderada)		documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso. 3. Analizar y actualizar el mapa de riesgos. 4. Informar a la Secretaría de Planeación y a Control Interno sobre el hallazgo y las acciones tomadas.
	Oficina de Control Interno	1. Informar al líder del proceso y al Secretario o Jefe de Oficina sobre la desviación encontrada. 2. Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso y ajustar el mapa de riesgos. 3. Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver la desviación. 4. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.
Riesgos de Gestión y Riesgos de Seguridad de la Información (Zona Baja)	Líder de Proceso	1. Establecer acciones correctivas al interior del proceso involucrado para mitigar el riesgo materializado. 2. Analizar y actualizar el mapa de riesgos para modificar la valoración del riesgo.
	Oficina de Control Interno	1. Informar al líder del proceso y al Secretario o Jefe de Oficina sobre la desviación encontrada. 2. Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso y ajustar el mapa de riesgos. 3. Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver la desviación. 4. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

13. SEGUIMIENTO AL RIESGO RESIDUAL

El seguimiento al riesgo residual lo realizará cada Secretario de Despacho o Jefes de Oficina, en compañía de los líderes de proceso, según periodicidad establecida en los formatos: "Mapa de Riesgos de Gestión" y "Mapa de Riesgos de Corrupción".

La Secretaría de Planeación realizará seguimiento trimestral a los Tableros de Riesgos y Controles de Gestión por dependencia, con el fin de elaborar un informe se seguimiento y presentarlo al Comité Institucional de Gestión y Desempeño.

La Oficina de Control Interno, se encargará de evaluar en forma independiente los Tableros de Riesgos y Controles definidos, así como su correspondiente seguimiento trimestral del Mapa de Riesgos de Corrupción.

14. ANEXOS

1. Decreto DAM 1100-122 del 10 de Septiembre del 2021
2. SIG.CT-01-F2 - Criterios para la calificación del Impacto de Riesgos de Corrupción.
3. SIG.CT-01-F3 "Matriz de Riesgos de Gestión 2022"
4. SIG.CT-01-F4 "Matriz de Riesgos de Corrupción 2022

Elaboró	Aprobó	Fecha
Secretaría de Planeación		

NOMBRE	FIRMA
DIRECTOR ADMINSITRATIVO	
SECRETARIO DE PLANEACIÓN	
SECRETARIO DE DESARROLLO INSTITUCIONAL	
SECRETARÍA DE HACIENDA	
JEFE OFICINA JURÍDICA	
OFICINA DE CONTROL INTERNO	
SECRETARÍA TIC	