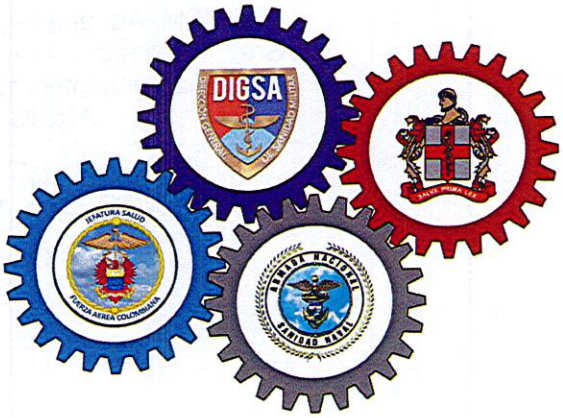
Guía para la Administración del Riesgo

SUBSISTEMA DE SALUD DE LAS FUERZAS MILITARES

Un equipo humano al servicio de la salud



CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Noviembre 2020	Versión Inicial.

CONTROL DE APROBACIÓN

Aprobó:	Mayor General JAVIER ALONSO DÍAZ GÓMEZ Director General de Sanidad Militar	
Revisó:	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección	
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG	PD. Monica Bibiana Bustamante Rondon Grupo Planeación Estratégica DIGSA Área Desarrollo Institucional ARDEI
	SMSM. Adriana Espinel Torres Grupo Planeación Estratégica DIGSA Área Sistemas Integrados de Gestión ARSIG	TS. Deysy Yanet Martínez Grupo Planeación Estratégica DIGSA Área Sistemas Integrados de Gestión ARSIG
Elaboró:	TASD. Nidia Liliana Guerrero Santos Grupo de Planeación Estratégica DIGSA Área Desarrollo Institucional ARDEI	

Tabla de contenido

1 Presentación

La Guía para la Administración del Riesgo es una herramienta e instrumento de trabajo del Subsistema de Salud de las Fuerzas Militares, que permite el fortalecimiento en la identificación y análisis de los riesgos que impiden alcanzar los objetivos institucionales que contribuyen en el mejoramiento continuo en la prestación del servicio. Es responsabilidad de cada Líder y/o Coordinador de Grupo, proceso o área del SSFM aplicar acciones, que seguramente no desaparecerán totalmente la amenaza o el riesgo, pero sí ayudarán a disminuir o mitigar su probabilidad de ocurrencia y su impacto.

2 Objetivo General

Emitir los lineamientos para la formulación, administración y monitoreo de los riesgos del Subsistema de Salud de las Fuerzas Militares, que se puedan derivar del aseguramiento y la prestación de los servicios de salud.

3 Alcance

Orientar a todos los actores del Subsistema de Salud de las Fuerzas Militares, para la administración del riesgo, teniendo como fundamentos la metodología definida por el Departamento Administrativo de la Función Pública -DAFP y la Norma Técnica Internacional ISO/31000:2018, contemplada como buenas prácticas en la Gestión del Riesgo.

4 Fundamento Normativo

Fecha	Descripción
Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. Art. 2. Objetivos del Sistema de Control Interno. a) Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan, Literal f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que pueden afectar el logro de los objetivos. 4 literal a): toda entidad debe establecer objetivos y metas tanto generales como específicas, así como la formulación de los Planes Operativos que sean necesarios.
Ley 352 de 1997	Por la cual se reestructura el Sistema de Salud y se dictan otras disposiciones en materia de Seguridad Social para las Fuerzas Militares y la Policía Nacional.
Ley 1474 de 2011	"Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" Capítulo VI. Políticas

Fecha	Descripción
	institucionales y pedagógicas. Artículo 73. Plan Anticorrupción y de Atención al Ciudadano. Artículo 74. Plan de Acción de las entidades Públicas.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1955 de 2019	Por la cual se expide el Plan Nacional de Desarrollo 2018 – 2022, Pacto por Colombia Pacto por la Equidad, marco normativo que servirá a este Gobierno para impulsar su propuesta de desarrollo
Decreto 2641 de 2012	"Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011". Artículo 7: Las entidades del orden nacional, departamental y municipal deberán publicar en un medio de fácil acceso al ciudadano su Plan Anticorrupción y de Atención al Ciudadano a más tardar el 31 de enero de cada año.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", Capítulo 3 Sistema Institucional y Nacional de Control Interno." Artículo 2.2.21.5.4 Administración de riesgos. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo.
Decreto 338 de 2019	"Por el cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción". Capítulo 7 Red Anticorrupción. Artículo 2.2.21.7.1. Creación de la Red Anticorrupción. Crease la Red Anticorrupción integrada por los Jefes de Control Interno o quien haga sus veces para articular acciones oportunas y eficaces en la identificación de casos o riesgos de corrupción en instituciones públicas, para generar las alertas de carácter preventivo frente a las decisiones de la administración, promoviendo la transparencia y la rendición de cuentas en la gestión pública.
Acuerdo No 36 de 2003 del CSSMP	"Por el cual se establecen políticas generales para orientar una efectiva gestión del SSMP"
Acuerdo No 37 de 2003 del CSSMP	"Por el cual se establecen normas para el control y evaluación de la gestión en el SSMP"
Norma Técnica Internacional ISO 31000:2018	"Gestión del Riesgo Principios y Directrices" ICONTEC Internacional.
Guía para la administración del riesgo y el diseño de controles en entidades públicas.	Riesgos de Gestión, Corrupción y Seguridad Digital, versión 4. Dirección de Gestión y Desempeño Institucional, octubre 2018. DAFP.

5 Marco Conceptual

CONCEPTO	DESCRIPCIÓN
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.

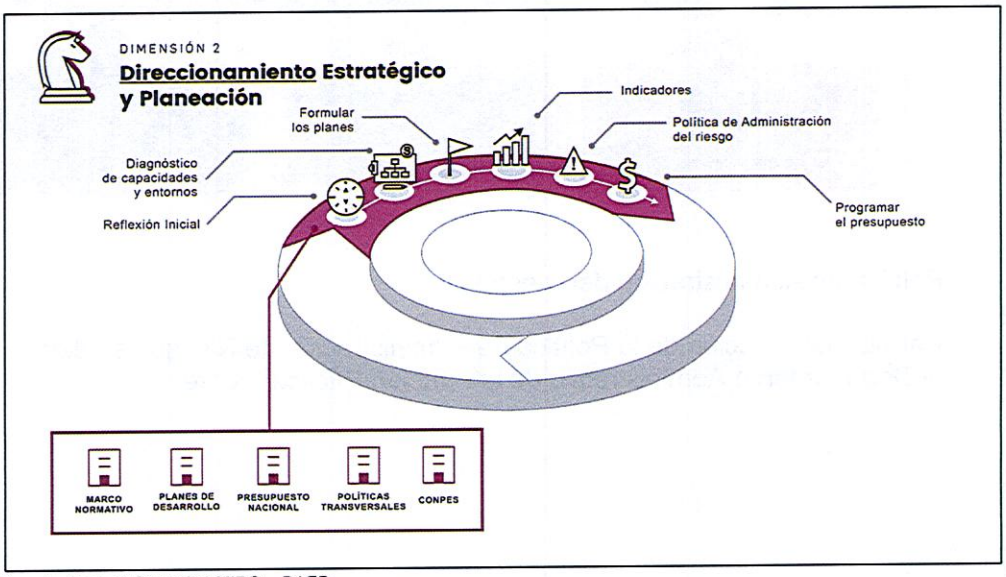
CONCEPTO	DESCRIPCIÓN
Riesgo de corrupción:	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgo de seguridad digital:	Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos 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.
Probabilidad:	Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
Riesgo residual:	Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
Impacto:	Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
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.
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.
Causa:	Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
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
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.
Confidencialidad:	Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
Control:	Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
Vulnerabilidad:	Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
Amenazas:	Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
Integridad:	Propiedad de exactitud y completitud.
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.
Contexto estratégico:	Son las condiciones externas e internas del entorno que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
Contexto Externo:	Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad.
Contexto Interno:	Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.

CONCEPTO	DESCRIPCIÓN
Contexto del Proceso:	Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.

6 Administración del Riesgo

Para el Subsistema de Salud de las Fuerzas Militares - SSFM es fundamental el adoptar y aplicar los lineamientos del Gobierno Nacional en marco legal como lo define el Departamento de la Función Pública en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas Versión 4 de octubre 2018; por lo tanto, el desarrollo de la Guía para la Administración del Riego del SSFM, define los mecanismos y acciones específicas que aportan a fortalecer el conocimiento y aplicación de la metodología para identificar, analizar, valorar, manejar y monitorear los riesgos actuales y futuros.

La administración del riesgo es la base para la planificación y contribución al cumplimiento de los objetivos estratégicos, para la implementación y mejora de los procesos en alineación con lo que establece el Modelo Integrado de Planeación y Gestión Dimensión 2 "Política de Administración del Riesgo":



Fuente: Manual Operativo MIPG – DAFP

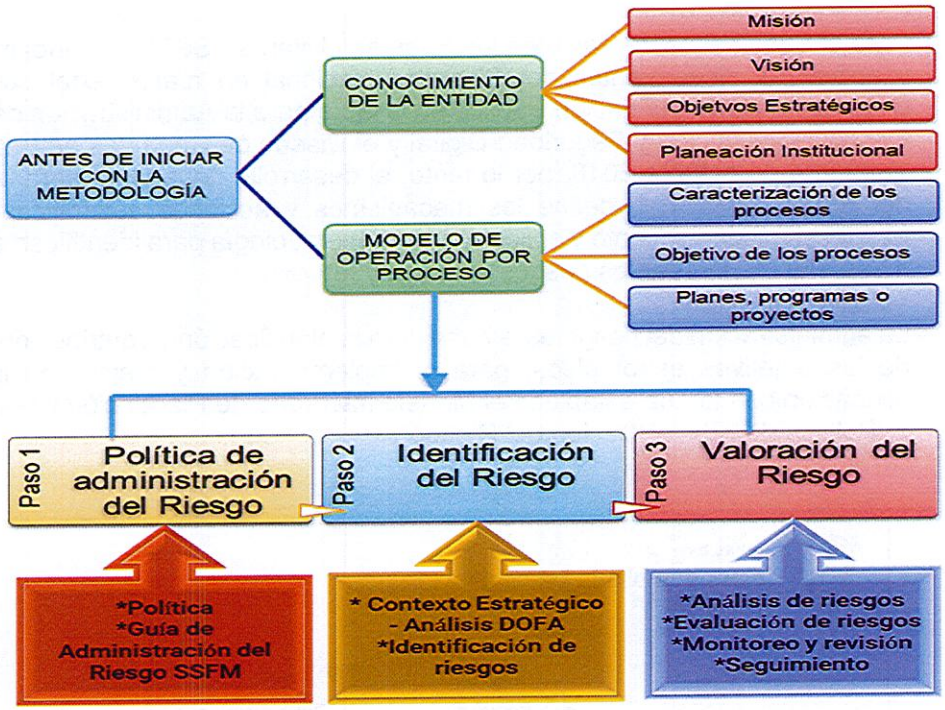
6.1 Estructura General - Metodología para la Administración del Riesgo

De acuerdo con el Departamento Administrativo de la Función Pública[1], para la adecuada aplicación de la metodología de la administración del riesgo, es indispensable conocer la

[1] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 13p.

entidad y el modelo de operación por procesos como se describe en el siguiente esquema:

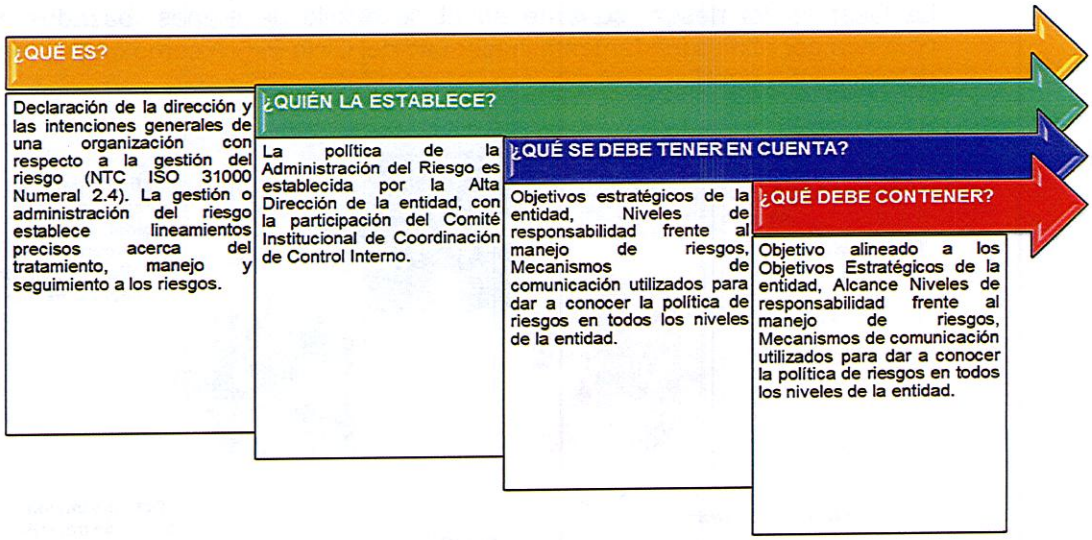
Metodología para la Administración del Riesgo



6.2 Política de Administración del Riesgo

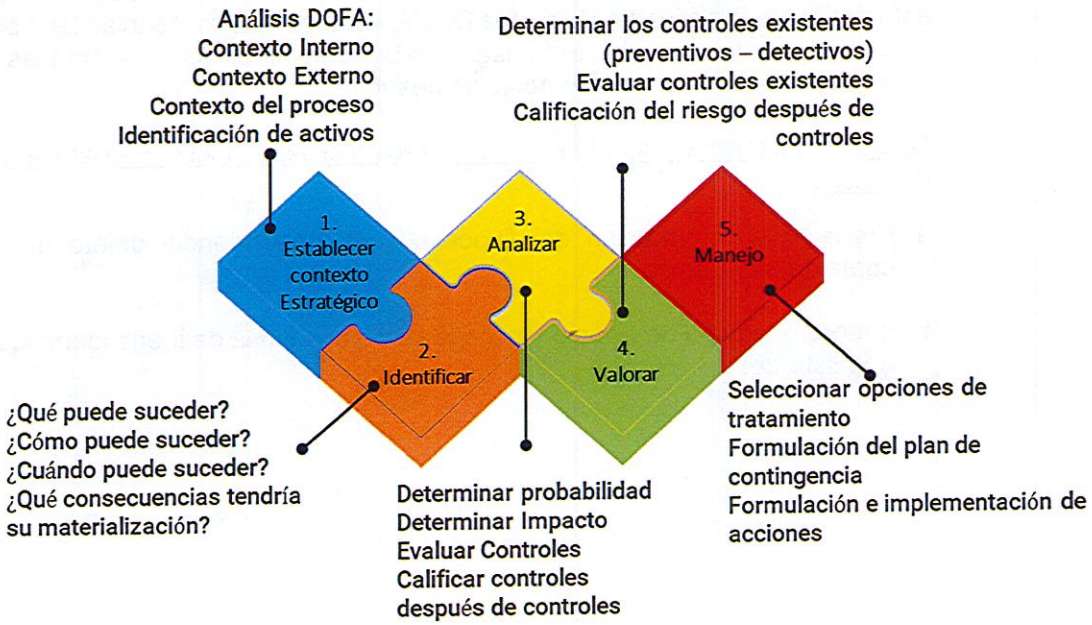
Para la construcción de la Política de Administración de Riesgos se debe precisar según el Departamento Administrativo de la Función Pública[2] sobre:

[2] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 14p.



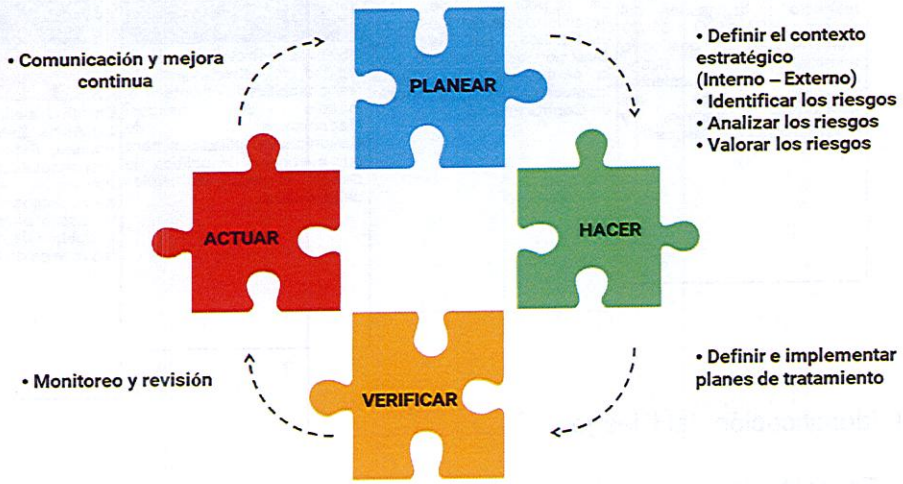
6.3 Identificación del Riesgo

En esta etapa se realiza la identificación de los riesgo que pueden llegar a afectar el cumplimiento de los objetivos institucionales, para ello es fundamentar definir el contexto estratégico, y así ejecutar cada uno de los pasaos definidos en la metodología.



6.3.1 Administración del Riesgo en el Ciclo PHVA

La Gestión del riesgo, consiste en el desarrollo de etapas, basados en la mejora continua por ello es fundamental hacer uso del Ciclo PHVA como insumo de la definición del contexto estratégico.



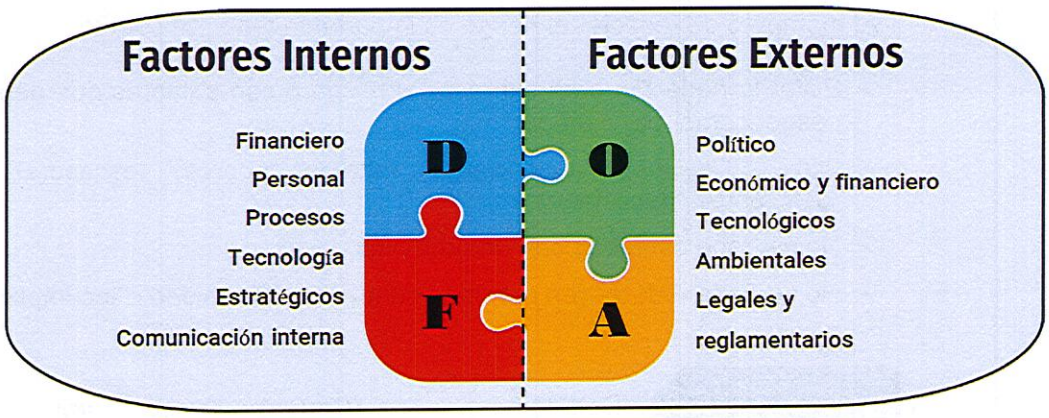
6.3.2 Contexto Estratégico:

Proporciona la información necesaria de la entidad, el proceso y sus interrelaciones, por lo que es necesario establecer los objetivos, las estrategias, el alcance y los parámetros de las actividades. La herramienta que permite la definición del contexto estratégico de la entidad es la matriz DOFA, en la cual se evidencian las oportunidades y amenazas externas, y las fortalezas y debilidades internas. Mediante las debilidades y amenazas se identifican los posibles riesgos.

Qué se debe tener en cuenta en la Elaboración de la Matriz DOFA para la identificación del riesgo

a) Preparar la información del Proceso y /o Dependencia objeto de análisis del contexto estratégico.

b) Integre el equipo de trabajo y por medio de una lluvia de ideas identifique y elabore una lista de:



c) Califique y de prioridad a las anteriores.

d) Revise el impacto en el proceso y defina los posibles riesgos.

Para el levantamiento del contexto estratégico se debe hacer uso del formato Diagnostico Estratégico DOFA DIGSA, versión vigente codificada en el Sistema Integrado de Gestión.

6.3.3 Identificación del Riesgo:

La identificación del riesgo debe ser permanente e interactiva, a partir del resultado del análisis del contexto estratégico. Para su desarrollo se debe tener en cuenta el conocimiento previo de situaciones que han o que pueden llegar a obstaculizar el cumplimiento de los objetivos.

Las preguntas claves para la identificación del riesgo:

a) ¿QUÉ PUEDE SUCEDER?[3] Identificar la afectación del cumplimiento del objetivo.

b) ¿CÓMO PUEDE SUCEDER?[4] Establecer las causas a partir de los factores determinados en el contexto.

c) ¿CUÁNDO PUEDE SUCEDER?[5] Revisar los procesos y procedimientos para identificar el momento.

d) ¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?[6] Determinar los posibles efectos del riesgo.

---

[3] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018.
[4] Ibid. p22
[5] Ibid. p22
[6] Ibid. p22

Al momento de redactar el riesgo es importante tener en cuenta:

- Evitar la negación para expresar el riesgo o con palabras que denoten factor de riesgo, como, por ejemplo:
- ✓ "No…", "Que no…" "ausencia de", "falta de", "poco(a)", "escaso(a)", "insuficiente", "deficiente", "debilidades en…"[7]
- No se debe confundir con un problema.
- No se debe redactar en términos de una inconformidad o incumplimiento.

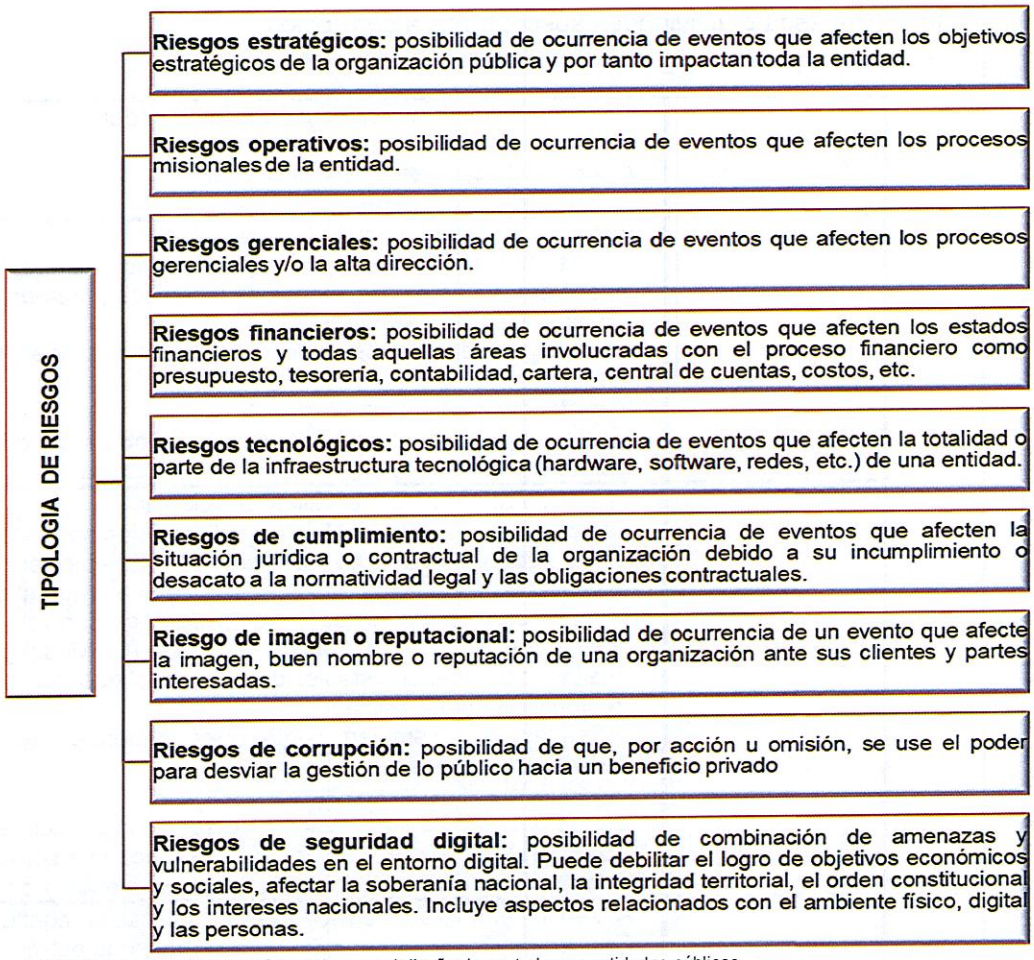
Frase para definir el riesgo

Debido a _____ **(Causa)** – Puede ocurrir _____ **Riesgo)** – lo que conllevaría a _____**consecuencia).**

6.3.4 Clasificación del Riesgo

Se debe definir la tipología del riesgo de acuerdo a las siguientes clases, como lo estipula el Departamento Administrativo de la Función Pública[8]:

[7] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 27p
[8] Ibid. p28



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas

Entre de las tipologías encontramos el riesgo de corrupción el cual se establece sobre procesos y cumple con los siguientes componentes:

La descripción del riesgo de corrupción debe ser de forma clara y precisa, de tal manera que no conlleve a imprecisiones o confusiones con la causa generadora de los mismos, se identifica anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo o en aquellos casos que se requiera[9].

[9] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 24p

6.3.5 Procesos o actividades susceptibles a corrupción

Direccionamiento o Estratégico	* Concentración de autoridad o exceso de poder. * Extralimitación de funciones. * Ausencia de canales de comunicación. * Amiguismo y clientelismo.
Financiero	* Inclusión de gastos no autorizados. * Inversiones de dineros públicos en entidades de dudosa solidez financiera, a cambio de beneficios indebidos para servidores públicos encargados de su administración. * Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. * Inexistencia de archivos contables. * Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica
Contratación	* Estudios previos o de factibilidad deficientes. * Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). * Disposiciones establecidas en los pliegos de condiciones que dirigen los procesos hacia un grupo en particular. (Ej. Media geométrica). * Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. * Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. * Urgencia manifiesta inexistente. * Otorgar labores de supervisión a personal sin conocimiento para ello. * Concentrar las labores de supervisión en poco personal. * Contratar con compañías de papel que no cuentan con Experiencia
Información y documentación	* Ausencia o debilidad de medidas y/o políticas de conflictos de interés. * Concentración de información de determinadas actividades o procesos en una persona. * Ausencia de sistemas de información. * Ocultar la información considerada pública para los usuarios. * Ausencia o debilidad de canales de comunicación * Incumplimiento de la Ley 1712 de 2014.
Investigación y sanción	* Ausencia o debilidad de canales de comunicación. * Dilatar el proceso para lograr el vencimiento de términos o la prescripción del mismo. * Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. * Exceder las facultades legales en los fallos.
Trámites y/o servicios internos y externos	* Cobros asociados al trámite. * Influencia de tramitadores * Tráfico de influencias: (amiguismo, persona influyente). * Demorar su realización.
Reconocimiento de un derecho	* Falta de procedimientos claros para el trámite. * Imposibilitar el otorgamiento de una licencia o permiso. * Ofrecer beneficios económicos para aligerar la expedición o para amañar la misma. * Tráfico de influencias: (amiguismo, persona influyente).

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – 32 y 33p.

6.4 Análisis del Riesgo

6.4.1 Descripción del Riesgo

Habiendo ya identificado y clasificado el riesgo, se procede a realizar el análisis del mismo, con el fin establecer las causas, consecuencias que potencialmente tendrían, la probabilidad e impacto del riesgo "Riesgo Inherente" y la evaluación del riesgo donde se define el grado de exposición.

Para la consolidación de los elementos del riesgo se debe hacer uso del formato mapa de riesgos institucional DIGSA, versión vigente codificada en el Sistema Integrado de Gestión.

PROCESO	NOMBRE DEL RIESGO	CLASIFICACION	DESCRIPCIÓN	CAUSAS	CONSECUENCIAS	RIESGO INHERENTE		
						PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Nombre del proceso establecido en el mapa de procesos de la entidad	Descripción resultado del análisis del contexto estratégico	Establecida por el proceso teniendo como herramienta la tipología del riesgo.	Características generales o las formas en que se observa o manifiesta el riesgo identificado	(factores internos, externos o de producto), medios, circunstancias, sujetos u objetos que pueden desencadenar la amenaza	Lo que podría suceder si se materializa el riesgo –efecto-; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes	Posibilidad de ocurrencia Puede ser medida con criterios de frecuencia,	Consecuencias que puede ocasionar a la organización	Resultado entre Probabilidad vs impacto

6.4.2 Analizar el Riesgo

Para efectos del análisis del riesgo se tomarán los niveles de probabilidad que se presentan en la siguiente tabla establecida por el Departamento Administrativo de la Función Pública[10]:

CRITERIOS PARA CALIFICAR LA 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.

Fuente: Criterios parar calificar la probabilidad - DAFP

[10] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 39p

A continuación, se presentan las especificaciones según la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital[11] de cada criterio para medir el impacto del riesgo según la calificación del riesgo (Gestión, Corrupción, Seguridad Digital):

a. *Riesgo de Gestión*[12]

CRITERIOS PARA CALIFICAR EL IMPACTO - RIESGO DE GESTIÓN				
NIVEL	ESCALA	DESCRIPCIÓN	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad	Impacto que afecte la ejecución presupuestal en un valor ≥50%.	Interrupción de las operaciones de la entidad por más de cinco (5) días.
			Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%.	Intervención por parte de un ente de control u otro ente regulador.
			Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%.	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.
			Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad	Impacto que afecte la ejecución presupuestal en un valor ≥20%.	Interrupción de las operaciones de la entidad por más de dos (2) días.
			Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%.	Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta
			Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%.	Sanción por parte del ente de control u otro ente regulador.
			Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las	Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno

[11] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 40p

[12] Ibid. p41 -

			cuales afectan en un valor ≥20% del presupuesto general de la entidad	Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad	Impacto que afecte la ejecución presupuestal en un valor ≥5%.	Interrupción de las operaciones de la entidad por un (1) día.
			Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%.	Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.
			Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%.	Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios
			Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	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.
2	Menor	Si el hecha llegara a presentarse, tendría bajo impacto o efecto sobre la entidad	Impacto que afecte la ejecución presupuestal en un valor ≥1%	Interrupción de las operaciones de la entidad por algunas horas
			Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%.	Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias.
			Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%.	Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos
			Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	
1	Insignificante	Si el hecha llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad	Impacto que afecte la ejecución presupuestal en un valor ≥0,5%.	No hay interrupción de las operaciones de la entidad.
			Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%.	No se generan sanciones económicas o administrativas.

			Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%.	No se afecta la imagen institucional de forma significativa.
			Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad	

b. Riesgo de Corrupción[13]

CRITERIOS PARA CALIFICAR EL IMPACTO - RIESGO DE CORRUPCIÓN			
No.	PREGUNTA SI EL RIESGO DE CORRUPCIÓN SEMATERIALIZA PODRÍA	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?		
	Total		

La respuesta afirmativa de la tabla define la escala en la que se ubica el impacto del riesgo de corrupción, así:

[13] Ibid. p46

ESCALA DE IMPACTO CON ENFOQUE DE CORRUPCIÓN		
Escala	Descripción	Respuestas Afirmativas
Moderado	Genera medianas consecuencias sobre la entidad	1 a 5
Mayor	Genera altas consecuencias sobre la entidad.	6 a 11
Catastrófico	Genera consecuencias desastrosas para la entidad	12 a 19

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos.

c. Riesgo de Seguridad Digital[14]

CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDA DIGITAL				
VALOR DEL IMPACTO	NIVEL	DESCRIPCIÓN	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad	✓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.
2	Menor	Si el hecho llegara a presentarse, tendría bajo consecuencias o efectos sobre la entidad	✓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.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad	✓ 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.

[14] Ibid. p42

CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDA DIGITAL				
VALOR DEL IMPACTO	NIVEL	DESCRIPCIÓN	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad	✓ 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 interés particular de los empleados y terceros.
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad	✓ 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.

El impacto cuantitativo establece variables para los riesgos de Seguridad Digital[15], las cuales se centran en:

VARIABLE	DEFINICIÓN
Confidencialidad, integridad y disponibilidad	De acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones
Población	Está asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectados por la materialización de algún riesgo en los activos identificados.

[15] Ibid. p43

VARIABLE	DEFINICIÓN
Presupuesto	Es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.
Ambiental	Alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital.

6.4.3 Matriz de Calificación, Evaluación y Respuesta a los Riesgos o Mapa de Calor

Consiste en una matriz con dos ejes, donde el eje X representa la probabilidad de frecuencia y el eje Y representa el impacto. Para establecer el nivel del Riesgo Inherente, este se ubica en un cuadrante en el punto de intersección resultante de la probabilidad y el impacto anteriormente definido con ayuda de las tablas de criterios.

PROBABILIDAD	ZONA DE RIESGO				
5 CASI SEGURO	ZONA DE RIESGO ALTA	ZONA DE RIESGO ALTA	ZONA DE RIESGO EXTREMA	ZONA DE RIESGO EXTREMA	ZONA DE RIESGO EXTREMA
4 PROBABLE	ZONA DE RIESGO MODERADA	ZONA DE RIESGO ALTA	ZONA DE RIESGO ALTA	ZONA DE RIESGO EXTREMA	ZONA DE RIESGO EXTREMA
3 POSIBLE	ZONA DE RIESGO BAJA	ZONA DE RIESGO MODERADA	ZONA DE RIESGO ALTA	ZONA DE RIESGO EXTREMA	ZONA DE RIESGO EXTREMA
2 IMPROBABLE	ZONA DE RIESGO BAJA	ZONA DE RIESGO BAJA	ZONA DE RIESGO MODERADA	ZONA DE RIESGO ALTA	ZONA DE RIESGO EXTREMA
1 RARA VEZ	ZONA DE RIESGO BAJA	ZONA DE RIESGO BAJA	ZONA DE RIESGO MODERADA	ZONA DE RIESGO ALTA	ZONA DE RIESGO EXTREMA
IMPACTO	1 INSIGNIFICANTE	2 MENOR	3 MODERADO	4 MAYOR	5 CATASTRÓFICO

Para los riesgos de corrupción solo aplican las columnas de impacto Moderado, Mayor y Catastrófico.

6.5 Valoración del Riesgo

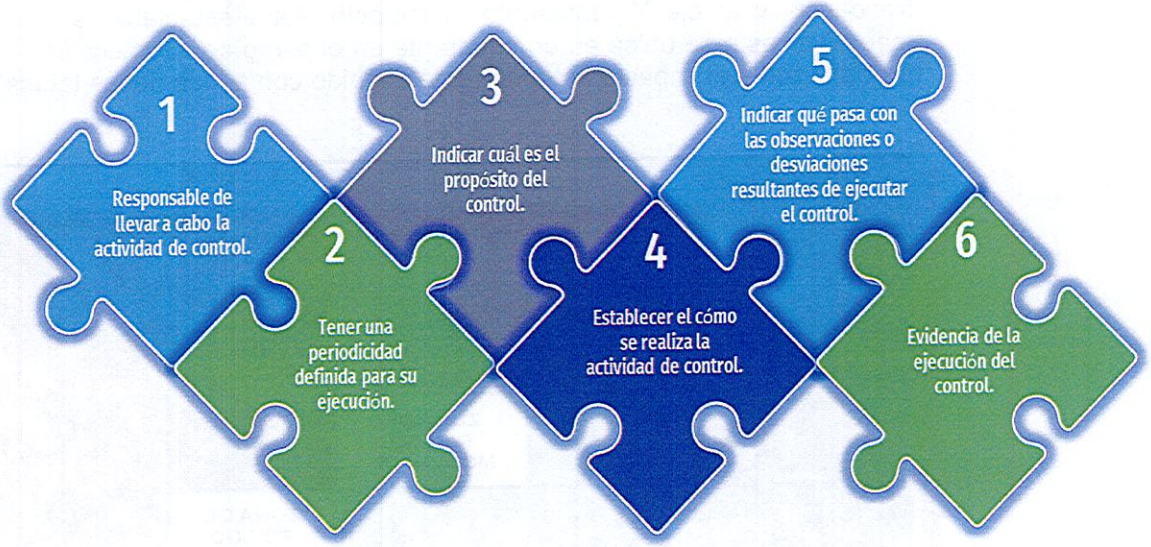
Permite comparar los resultados de su calificación en términos de probabilidad e impacto, para tener un primer resultado cuantitativo y cualitativo del estado actual del riesgo sin haber tomado acción alguna para su manejo y así, posteriormente, poder tomar decisiones y definir los controles a ejecutar con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE) y confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL), teniendo en cuenta los siguientes aspectos:

6.5.1 Valoración de los controles – diseño de controles

a. Descripción del Control:

Los controles corresponden a las medidas de tratamiento que permiten modificar el riesgo, porque actúan sobre alguna de las dos variables de su medición (probabilidad o impacto), bien sea para detectarlo a tiempo (evitar que se materialice) o reducirlo (minimizar las consecuencias).

b. Como se define un control[16]:



c. Clase de Control:

Los controles se deben clasificar de acuerdo a su naturaleza, así:

- ✓ Preventivos: Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización
- ✓ Correctivos: Aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

c. Características del control:

- Oportunidad: Debe ser aplicado en el momento adecuado respecto al evento que se espera controlar.

[16] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 49p.

- Economía (Costo – Beneficio): No debe superar el beneficio derivado de su aplicación, su representación en tiempo y dinero debe justificarse con las ventajas reales de los resultados que se obtengan.

- Significancia: Debe corresponder con actividades importantes dentro del proceso y no con cuestiones sin trascendencia.

- Operatividad: Debe ejecutarse con facilidad sin crear confusiones.

- Apego jurídico: Debe estar sujeto a la legislación que rige a la Institución y subordinado al principio de legalidad.

- Funcionalidad: Debe guardar estrecha relación con los riesgos asociados a través de su objetivo, es decir se debe tener claridad en cuanto a qué se busca con la aplicación de dicho control.

- Viabilidad técnica: Debe estimar si es posible que el control se ejecute con las condiciones tecnológicas, conocimientos y herramientas disponibles.

6.5.1.1 Evaluación de los Controles:

Los criterios para la evaluación de los controles están directamente relacionados con los 6 pasos anteriores, a partir de la respuesta se dará una calificación en el seguimiento que se realice teniendo en cuenta la tabla definida por el Departamento Administrativo de la Función Pública[17]:

ANÁLISIS Y DISEÑO DE CONTROLES			
Criterio de evaluación	Aspecto a evaluar en el diseño del control	Opciones de respuesta y Peso evaluación	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado = 15	No Asignado = 0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado = 15	Inadecuado = 0
2. Periocidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna = 15	Inoportuna = 0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si solas prevenir o detectar las causas que puedan dar origen al riesgo, El: Verificar, calidad, cotejar, comprar, revisar, etc.	Prevenir = 15 Detectar = 10	No es un control = 0

[17] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 60-61p.

ANÁLISIS Y DISEÑO DE CONTROLES			
Criterio de evaluación	Aspecto a evaluar en el diseño del control	Opciones de respuesta y Peso evaluación	
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable = 15	No Confiable = 0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultado de la ejecución del control son investigadas y resueltas de manera oportuna?	Se Investigan y resuelven oportunamente = 15	No se Investigan y resuelven oportunamente = 0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa = 15	Incompleta / no Existe = 0

6.5.1.2 Resultados de la Evaluación en el diseño y ejecución del Control[18]:

Inmediatamente evaluados los controles de acuerdo a la tabla anterior (Análisis y diseño de controles), se deberá realizar la sumatoria de los valores numéricos, para determinar la calificación del diseño. Posteriormente, el responsable del proceso deberá llevar a cabo una autoevaluación, en donde confirmará la ejecución de estos controles.

Esta evaluación determinará los resultados del riesgo, de acuerdo con la siguiente tabla:

Resultados de la evaluación del riesgo		
Rango de Calificación del Diseño	Resultado - evaluación del diseño del control	Resultado - ejecución del control
Fuerte	Calificación entre 96 y 100	El control se ejecuta de manera consistente por parte del responsable (siempre)
Moderado	Calificación entre 86 y 95	El control se ejecuta algunas veces por parte del responsable (algunas veces)
Débil	Calificación entre 0 y 85	El control no se ejecuta por porta del responsable (nunca)

Deben cumplirse todas las variables para que un control se evalúe como bien diseñado. Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 86%, se debe establecer un plan de contingencia que permita tener un control o controles bien diseñados.

6.5.1.3 Solidez Individual de los Controles[19]

[18] Ibid. p62
[19] Ibid. p63

Se calculará la solidez individual de los controles, teniendo en cuenta las dos variables, por lo que siempre la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, de acuerdo con la siguiente tabla:

ANÁLISIS Y EVALUACIÓN DE LOS CONTROLES PARA LA MITIGACIÓN DEL RIESGO			
Peso del diseño de cada control	Peso de la ejecución de cada control	Solidez individual de cada control Fuerte: 100 Moderado: 50 Débil: 0	Debe establecer acciones para fortalecer el control SÍ / NO
Fuerte Calificación entre 96 y 100	Fuerte (Siempre se ejecuta)	Fuerte + Fuerte = Fuerte	No
	Moderado (Algunas veces)	Fuerte + Moderado = Moderado	Si
	Débil (no se ejecuta)	Fuerte + Débil = Débil	Si
Moderado Calificación entre 86 y 95	Fuerte (Siempre se ejecuta)	Moderado + Fuerte = Moderado	Si
	Moderado (Algunas veces)	Moderado + Moderado = Moderado	Si
	Débil (no se ejecuta)	Moderado + Débil = Débil	Si
Débil Calificación entre 0 y 85	Fuerte (Siempre se ejecuta)	Débil + Fuerte = débil	Si
	Moderado (Algunas veces)	Débil + Moderado = Débil	Si
	Débil (no se ejecuta)	Débil + Débil = Débil	Si

6.5.1.4 Solidez del Conjunto de Controles:[20]

Teniendo los resultados de la solidez individual de cada control, se procederá a definir la solidez del conjunto de controles para cada riesgo. Para esto, se debe identificar el promedio de los valores numéricos de la solidez individual de cada control determinado al riesgo, de la siguiente manera:

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez individual de los controles es igual a 100.
Moderado	El promedio de la solidez individual de los controles está entre 50 y 99.
Débil	El promedio de la solidez individual de los controles es menor a 50

Sí el resultado de la calificación de la autoevaluación de los controles está por debajo de 50, se debe formular una Plan de contingencia o acción correctiva.

6.5.2 Riesgo Residual[21]

Es importante denotar que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para

[20] Ibid. p64
[21] Ibid. p66

el cálculo del riesgo residual depende del resultado obtenido de la evaluación del diseño y ejecución de los controles, los riesgos podrán desplazarse en la matriz de calor, de acuerdo con la tabla que se presenta a continuación:

DESPLAZAMIENTO DE LA PROBABILIDAD Y DEL IMPACTO				
Solidez del conjunto de los controles	Controles ayuda a disminuir la probabilidad	Controles ayudan a disminuir impacto	Niveles de disminución de probabilidad	Niveles de disminución de impacto
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No disminuye	1	0
Moderado	No disminuye	Directamente	0	1

La mayoría de los controles que se diseñan son para disminuir la probabilidad de que ocurra una causa o evento que pueda llevar a la materialización del riesgo y muy pocos son dirigidos al impacto.

El desplazamiento y/o disminución para los de riesgos de corrupción solo designa para la probabilidad. Es decir, para el impacto no aplica el desplazamiento.

En aquellos casos donde el resultado de la evaluación del diseño y ejecución de los controles, arroja que la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

6.6 Manejo o Tratamiento del Riesgo:

Está claro que no todos los riesgos tienen el mismo nivel de criticidad y que su gestión implica una serie de esfuerzos y costos en los que debe incurrir la entidad, de ahí la importancia que los líderes de proceso (primera línea de defensa) evalúen las opciones existentes en materia de tratamiento del riesgo para la mitigación de los riesgos de Gestión, Corrupción y Seguridad Digital, así como la relación costo-beneficio de las medidas de tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo.

Por lo anterior se deberá seleccionar una sola de las siguientes opciones de tratamiento definidas en la Guía del Departamento Administrativo de la Función Pública[22]:

[22] Departamento Administrativo de la Función Pública. Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital. Versión 4. Bogotá, Colombia. 2018. 68p.

6.6.1 Plan de Contingencia

Le corresponde a la primera línea de defensa establecer el Plan de Contingencia el cual ayudará a controlar una situación de materialización del riesgo y a minimizar los impactos o efectos negativos que este pueda ocasionar. Estos son dinámicos y cuando se definan deben ser revisados anualmente para verificar su pertinencia frente al riesgo.

La materialización de un riesgo obliga a activar el plan de contingencia (el cual se encuentra en estado suspendido en la Plataforma Suite Visión Empresarial) solicitando dicha acción al Grupo de Planeación Estratégica de la entidad quien cumple con la función de administrador de los planes, o de ser el caso que el proceso no cuente con dicho plan, deberá crear la respectiva acción correctiva en el módulo de Mejoras en la SVE y relacionarla en el riesgo que se materializó.
Aquellas actividades necesarias que contengan los planes de contingencia deberán contribuir para que se realice la investigación de la materialización y describir las actividades requeridas para dar continuidad con las funciones y responsabilidades afectadas.

La formulación del Plan de contingencia, debe ir acorde al formato Plan de Contingencia DIGSA, versión vigente codificada en el Sistema Integrado de Gestión.

6.6.2 Actividades de Control

Son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

6.6.3 Acciones Asociadas

Durante la formulación del plan de acción de cada vigencia se deben definir acciones preventivas y/o de mitigación que ataquen la materialización de los riesgos de Gestión,

Corrupción y Seguridad Digital, los cuales pueden influir negativamente en el logro de los objetivos estratégicos y de los procesos; que permitan la correcta identificación, análisis, valoración y manejo de estos, siendo coherentes con los controles programados para los riesgos.

a. Acciones a seguir en caso de materialización de riesgos de corrupción

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

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.

2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.

3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.

4) Llevar a cabo un monitoreo permanente.

6.7 Monitoreo y Seguimiento

La entidad debe asegurar el logro de los objetivos, interesándose por el monitoreo y seguimiento periódico de los riesgos de la entidad (impactos, amenazas, vulnerabilidades y probabilidades), en busca de posibles cambios que requieran la valoración; esta acción debe ser realizada por el responsable o gestor de calidad, anexando sus debidas evidencias de acuerdo a lo establecido en los controles.

Los riesgos son dinámicos, por tanto, podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión o monitoreo periódico según su tipología:

TIPOLOGÍA	MONITOREO
Gestión	Trimestral
Corrupción	Bimestral
Seguridad Digital	Trimestral

6.7.1 Roles para Monitorear y Revisar la Gestión de Riesgos

El monitoreo y revisión de la gestión de riesgos está alineado con la dimensión del MIPG en la dimensión 7 "Control interno", que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad como sigue[23]:

[23] Departamento Administrativo de la Función Pública. Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 75p.

NIVEL	ROL	RESPONSABILIDAD
Estratégico	Alta Dirección Comité Coordinador de Control Interno	Definir el marco general de gestión del riesgo y el control y supervisar su cumplimiento.
Proceso	Líderes de Proceso Gestores	Gestionar los riesgos de proceso y de corrupción que pueden afectar el cumplimiento de los objetivos a través de (Identificación, análisis, evaluación, tratamiento y monitoreo de riesgos).
Acompañamiento	Grupo de Planeación Estratégica	Asistir y guiar a los procesos en la gestión adecuada de los riesgos que pueden afectar el logro de los objetivos, a través del establecimiento de directrices y del acompañamiento para: Identificación, análisis, evaluación, tratamiento y monitoreo de riesgos.
Seguimiento	Grupo de Seguimiento y Evaluación - cumple las funciones de Oficina de Control Interno (Auditorías internas)	Proveer aseguramiento independiente y objetivo sobre la efectividad de la gestión del riesgo validando que el nivel estratégico y de apoyo cumpla sus responsabilidades en la gestión del riesgo.

a. Línea Estratégica[24]:

Está conformada por el Director General de la entidad y Grupo del STAFF, quienes por medio del comité deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos, aplicando el esquema de responsabilidades, así:

LÍNEA ESTRATÉGICA	
Revisar los cambios en el Direccionamiento Estratégico y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados.	Revisión de la alineación de los objetivos estratégicos a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.
Hacer seguimiento en el Comité de Control Interno a la implementación de cada una de las Etapas de la Gestión del Riesgos y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.	Revisar el cumplimiento a los objetivos estratégicos y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
Hacer seguimiento y pronunciarse semestralmente sobre el riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo con la política de administración del riesgo establecida y aprobada.	Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción y seguridad digital, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
Revisar los planes de contingencia establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.	

[24] Ibid, p75

b. Primera Línea de Defensa[25]:

Forman parte los Líderes de Proceso, Gerentes de proyectos y Coordinadores deben monitorear y revisar el cumplimiento de los objetivos estratégicos y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción y Seguridad digital, desempeñando el rol de:

PRIMERA LÍNEA DE DEFENSA	
Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso	Revisión como parte de sus actividades de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.	Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos
Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción y seguridad digital, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.	Revisar los planes de contingencia establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos
Revisar y hacer seguimiento al cumplimiento de las actividades y planes de mejora acordados con la Línea Estratégica, Segunda y Tercer Línea de Defensa con relación a la Gestión de Riesgos.	

c. Segunda Línea de Defensa[26]

Está compuesta por los servidores públicos (Gestores) con responsabilidades directas de monitoreo, evaluación y seguimiento, deben monitorear y revisar el cumplimiento de los objetivos estratégicos y de procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción y seguridad digital, cumpliendo con el rol de:

SEGUNDA LÍNEA DE DEFENSA	
Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos pueda generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.	Revisión de la adecuada definición y alineación de los objetivos estratégicos a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.

[25] Ibid, p77-78
[26] Ibid. p79

SEGUNDA LÍNEA DE DEFENSA	
Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.	Revisar el riesgo inherente y residual por cada proceso, consolidar y pronunciarse sobre cualquier riesgo que este por fuera de los rangos de aceptación de la entidad.
Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.	Revisar los planes de contingencia 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.

d. Tercera Línea de Defensa[27]

La Oficina de Control Interno o quien haga sus veces como indica el Departamento de la Función Pública, es quien cumple con la función de revisar de manera independiente y objetiva el cumplimiento de los objetivos estratégicos y de procesos, a través de la adecuada gestión de los riesgos de Gestión, Corrupción y Seguridad Digital, su rol es:

TERCERA LÍNEA DE DEFENSA	
Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.	Revisión de la adecuada definición y alineación de los objetivos estratégicos a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción y seguridad digital.	Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.
Revisar el riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del rango de tolerancia del riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.	Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora establecidos como resultados de las auditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos.

6.8 Seguimiento

Uno de los roles que reglamentariamente desarrolla la Coordinación de Seguimiento y Evaluación es el de "Evaluar la Gestión del Riesgo" como tercera línea de defensa, proporcionando a la Alta Dirección información relacionada con la efectividad del Sistema de Control Interno, basado en las actuaciones de la primera y segunda línea de

[27] Ibid. p80

defensa; mediante el proceso de auditoría se verificará cómo opera la gestión del riesgo de la entidad, brindando información que permita a la primera línea tomar decisiones de carácter estratégico, proteger los recursos y minimizar riesgos que puedan afectar el cumplimiento de los objetivos. En cuanto al seguimiento de los riesgos de corrupción se deben tener en cuenta los siguientes puntos:

a) 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[28].

b) Primer seguimiento[29]: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

c) Segundo seguimiento[30]: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

d) Tercer seguimiento[31]: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

[28] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4. Bogotá, Colombia. 2018. 87p.
[29] Ibid, p87
[30] Ibid, p87
[31] Ibid, p87

7 Bibliografía

Departamento Administrativo de la Función Pública. (2011). Guía para la Administración del Riesgo.

Departamento Administrativo de la Función Pública. (Versión 4 octubre 2018). Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas

Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC. Norma Técnica Colombiana NTC/ISO/31000(2018). Gestión del Riesgo. Bogotá D.C.