Política de Administración del Riesgo

CUERPO OFICIAL DE BOMBEROS DE DOSQUEBRADAS

Fecha de vigencia: Julio de 2023

Contenido

1. INTRODUCCIÓN

Con la entrada en vigencia del nuevo modelo integrado de planeación y gestión (MIPG) – Decreto 1499 de 2017, el cual integró los Sistemas de Gestión de Calidad y de Desarrollo Administrativo creando un único sistema de gestión y su articulación con el Sistema de Control Interno, es fundamental para el Cuerpo Oficial de Bomberos de Dosquebradas fortalecer la gestión del riesgo conforme a los nuevos lineamientos del MIPG.

El propósito principal de este modelo es garantizar en las entidades públicas una mejor gestión para mejorar las condiciones de vida y generar mayor valor público en términos de bienestar, prosperidad y fortalecer la lucha contra la corrupción, en este sentido se hace necesario mejorar los controles en todos los niveles de la entidad que permita el logro de los objetivos establecidos.

Adicionalmente el crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, de lo cual nuestra entidad no es ajena, implican un alto riesgo dado lo importancia del activo que se maneja con ellas y dada su aplicación para un mejor servicio al ciudadano situación que obliga también a generar políticas de seguridad digital que permitan minimizar el riesgo en su uso, generando confiabilidad e integridad de la información, como también la disponibilidad de esta y la rapidez en los trámites asegurando la seguridad y la defensa de nuestra entidad.

Es por esto que, a partir de la presente política de gestión del riesgo, la entidad contará con una herramienta metodológica para identificar, valorar, definir controles frente a los riesgos de corrupción, riesgos de gestión, riesgos de seguridad de la información, riesgos de seguridad y salud en el trabajo
y riesgos en los procesos de contratación.

Fortalecer la gestión del riesgo permitirá que la entidad evalúe aquellos eventos negativos tanto internos como externos que puedan afectar o impedir el logro de los objetivos institucionales o identificar aquellos eventos positivos que se traduzcan en oportunidades para un mejor cumplimiento de su función.

2. PRESENTACIÓN

Teniendo en cuenta la nueva guía metodológica del DAFP V6 de noviembre de 2022, la entidad a través de los procesos de sistemas integrados de gestión, gestión de recursos tecnológicos y de la información (tecnologías), gestión de seguridad y salud en el trabajo y el proceso de gestión de control evaluación, estructura la siguiente política con el fin de fortalecer la gestión del riesgo en la entidad y así propender por el logro de los objetivos institucionales.

Las metodologías que se plantean, pretenden establecer para cada tipo de riesgo, mecanismos para identificar, valorar los riesgos, así como también establecer criterios frente al diseño e implementación de los controles de tal manera que éstos realmente estén orientados a reducir la(s) causa(s) que pueden ocasionar la materialización de los riesgos.
El propósito final es minimizar los riesgos a los que constantemente está expuesta nuestra entidad, fortaleciendo así el sistema de gestión que se está operando mediante el modelo integrado de planeación y gestión.

3. OBJETIVO

Establecer las metodologías frente a la administración de riesgos que seguirá el Cuerpo Oficial de Bomberos de Dosquebradas, en cuanto a la identificación, valoración, diseño de controles, seguimiento y evaluación y definición de responsabilidades en marco de las líneas defensa - Dimensión 7 – Control Interno del Modelo Integrado de Planeación y Gestión.

4. ALCANCE

La administración de riesgos del Cuerpo Oficial de Bomberos de Dosquebradas, estará fundamentada en el modelo de operación por Procesos, es por esta razón que esta política para la gestión del riesgo, es aplicable a todos los procesos de la empresa -incluyendo los tercerizados-, por consiguiente, aplica a todos los espacios físicos donde se desarrollen actividades en nombre de COBD y a todos los funcionarios y contratistas de la empresa.

Procesos del Cuerpo Oficial de Bomberos de Dosquebradas:

Procesos estratégicos	● Gestión estratégica ● Gestión de calidad
Procesos misionales	● Atención de emergencias ● Servicios complementarios
Procesos de apoyo	● Gestión administrativa
Procesos de control y evaluación	● Control de gestión

5. NIVELES DE ACEPTACIÓN DEL RIESGO – TOLERANCIA AL RIESGO

El nivel de aceptación del riesgo en la entidad se determinará posterior a la evaluación de los mapas de riesgos de cada uno de los procesos, es importante resaltar que los riesgos aceptables podrán ser aquellos que, calificando su probabilidad e impacto, y posterior a la definición de los controles quedan en una Zona de Riesgo Residual Baja. Para estos riesgos

aceptables en la entidad, no será necesario definirles un plan de acción. Es importante tener en cuenta que igualmente, debe existir un seguimiento continuo al riesgo.

Los riesgos de corrupción son catalogados como ***INACEPTABLES.***

6. TÉRMINOS Y DEFINICIONES

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.

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.

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales.

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 y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

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 la cuales se puede presentar el riesgo.

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

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

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

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado.

Gestor público: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales.

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

Integridad: Propiedad de exactitud y completitud.

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 poder ser 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.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

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

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele

considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo de Seguridad y salud en el trabajo: Combinación de la probabilidad de que ocurra un(os) evento(s) o exposición(es) peligroso(s), y la severidad de lesión o enfermedad, que puede ser causado por el (los) evento(s) o la(s) exposición(es).

Riesgo Fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

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.

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

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.

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

Fuentes:
1. Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.
2. GTC 45 Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional 2012-06-20.

Otras definiciones:

Conflicto de Intereses: En Colombia, el concepto conflicto de intereses se encuentra definido en el artículo 40 del Código Único Disciplinario –Ley 734 de 2002– y el artículo 11 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo –Ley 1437 de 2011–, los cuales señalan que el conflicto surge “cuando el interés general propio de la función pública entra en conflicto con el interés particular y directo del servidor público”. No obstante, existen otras definiciones complementarias a este enfoque legal que amplían el marco de referencia y que son útiles para orientar la identificación del conflicto de intereses y su declaración como mecanismo de gestión preventivo del comportamiento de los servidores públicos.

En este sentido la OCDE (2017)1 define el conflicto de intereses como “un conflicto entre las obligaciones públicas y los intereses privados de un servidor público, en el que el servidor público tiene intereses privados que podrían influir indebidamente en la actuación de sus funciones y sus responsabilidades oficiales”.

Información: Datos relacionados que tienen significado para la entidad. La información es un

activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Sistema de Gestión de la Seguridad y Salud en el Trabajo: SG-SST. El Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST consiste en el desarrollo de un proceso lógico y por etapas, basado en la mejora, continua y que incluye la política, la organización, la planificación, la aplicación, la evaluación, la auditoría y las acciones de mejora con el objetivo de anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y la salud en el trabajo.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

7. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

7.1 RESPONSABILIDADES DE LAS LÍNEAS DE DEFENSA EN MARCO DE LA GESTIÓN DEL RIESGO:

"El Modelo de las Líneas de Defensa" en marco del modelo integrado de planeación y gestión (MIPG) establece los roles y responsabilidades frente a los diferentes componentes del Sistema de Control Interno.

Uno de los componentes del sistema de control interno es la evaluación del riesgo, como proceso dinámico e interactivo que le permite a la entidad identificar, evaluar y gestionar aquellos eventos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales.

La gestión del riesgo en su integralidad está alineada con la dimensión número siete (7) del MIPG - "Control Interno", que se desarrolla a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad de la siguiente manera:

7.2 LÍNEA ESTRATÉGICA

- Define el marco general para la gestión del riesgo y el control.
- Está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.
- Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos (objetivos, metas, indicadores).
- En consecuencia, tiene la responsabilidad de definir el marco general para la gestión del riesgo y garantiza el cumplimiento de los planes en la entidad.

Responsabilidades según herramienta de autodiagnóstico:

- Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad
- Establecer la Política de Administración del Riesgo
- Asumir la responsabilidad primaria del Sistema de Control Interno y de la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo
- Específicamente el Comité Institucional de Coordinación de Control Interno, evaluar y dar línea sobre la administración de los riesgos en la entidad
- Realimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. Así mismo, hacer seguimiento a su gestión, gestionar los riesgos y aplicar los controles.

Responsabilidades frente a los riesgos de seguridad digital:

En materia de seguridad digital la entidad debe disponer de los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad digital, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad digital.

Se establecerá un marco de gestión de riesgos de seguridad digital que permitirá la identificación de amenazas y vulnerabilidades a las que la entidad pueda estar expuesta desde el entorno informático, con el fin de fortalecer el ambiente de control.

La línea estratégica o alta dirección debe asignar entre otros, recursos tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad digital.
- Recursos económicos para la implementación de controles de mitigación de riesgos (con base al análisis de riesgo realizado).
- Recursos para los aspectos de mejora continua, monitoreo y auditorías

El Cuerpo Oficial de Bomberos de Dosquebradas debe identificar todos los activos de información (se incluyen los que corresponden a las ICC) y se clasifican de acuerdo con la normatividad vigente y aplicable teniendo en cuenta las Leyes 1712 de 2014 y 1581 de 2012, que determinan la importancia del activo para la entidad e identifica el nivel de criticidad.

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debe llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

Se definen como activos de información elementos tales como: Aplicaciones de la organización, servicios web, redes, Información física o digital, tecnologías de información TI, Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital, por esto es que la entidad deberá contar con un inventario de activos de información que permita saber qué es lo que se debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano aumentando la confianza en el uso del entorno digital

7.3 PRIMERA LÍNEA DE DEFENSA

- A cargo de los gerentes públicos y líderes de los procesos o gerentes operativos de programas y proyectos de la entidad.
- Se encarga del mantenimiento efectivo de controles operativos ejecutar procedimientos de riesgo y el control sobre una base del día a día. La gestión operacional identifica, evalúa, controla y mitiga los riesgos.
- Son responsables de implementar acciones correctivas, igualmente detecta las deficiencias de control.

Responsabilidades según herramienta de autodiagnóstico:

- Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales
- Definen y diseñan los controles a los riesgos
- A partir de la política de administración del riesgo, establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección. Con base en esto, establecen los mapas de riesgos
- Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos. Implementan procesos para identificar, disuadir y detectar fraudes; y revisan la exposición de la entidad al fraude con el auditor interno de la entidad.

Responsabilidades frente a los riesgos de seguridad digital

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.

7.4 SEGUNDA LÍNEA DE DEFENSA

- A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: jefes de planeación, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, comité de enlaces operativos, áreas financieras, área de tic, entre otros que generen información para el aseguramiento de la operación
- Asegurar que los controles y procesos de gestión del riesgo de la 1era línea de defensa sean apropiados y funcionen correctamente, relacionados por el tema por el cual responde.
- Ejerce el control y la gestión de riesgos, las funciones de cumplimiento, seguridad, calidad, SST, entre otros.
- Supervisa la implementación de prácticas de gestión de riesgo eficaces por parte de la 1era línea y ayuda a los responsables de riesgos a distribuir la información adecuada sobre riesgos a todos los servidores de la entidad.
- Referente al tema de Conflicto de intereses serán los procesos de Gestión Jurídica y Gestión de Talento Humano los responsables de identificar y controlar los riesgos relacionados con dicho tema, evidenciando su implementación y control en los Mapas de Riesgos de Corrupción.
- Respecto a los riesgos de SST será el proceso de Gestión de Talento Humano el responsable de liderar la identificación, evaluación y control de los riesgos relacionados con dicho tema.

Responsabilidades según herramienta de autodiagnóstico

- Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada
- Asegurar que las evaluaciones de riesgo y control incluyan riesgos de fraude
- Ayudar a la primera línea con evaluaciones del impacto de los cambios en el SCI
- Monitorear cambios en el riesgo legal, regulatorio y de cumplimiento
- Consolidar los seguimientos a los mapas de riesgo
- Establecer un líder de la gestión de riesgos para coordinar las actividades en esta materia
- Elaborar informes consolidados para las diversas partes interesadas
- Seguir los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar
- Los supervisores e interventores de contratos deben realizar seguimiento a los riesgos de estos e informar las alertas respectivas

7.5 TERCERA LÍNEA DE DEFENSA

- A cargo de la Oficina de control interno, auditoría interna o quien haga sus veces.
- Proporciona información sobre la efectividad del S.C.I., la operación de la primera y segunda línea de defensa con un enfoque basado en riesgos.
- La función de la auditoría interna, a través de un enfoque basado en el riesgo, proporciona aseguramiento sobre la eficacia de gobierno, gestión de riesgos y control interno a la alta dirección de la entidad, incluidas las maneras en que funciona la primera y segunda línea de defensa.
- Orienta la elaboración del mapa de aseguramiento y evalúa la gestión de las segundas líneas de defensa

Responsabilidades según herramienta de autodiagnóstico

- Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa
- Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna
- Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías
- Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad
- Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas

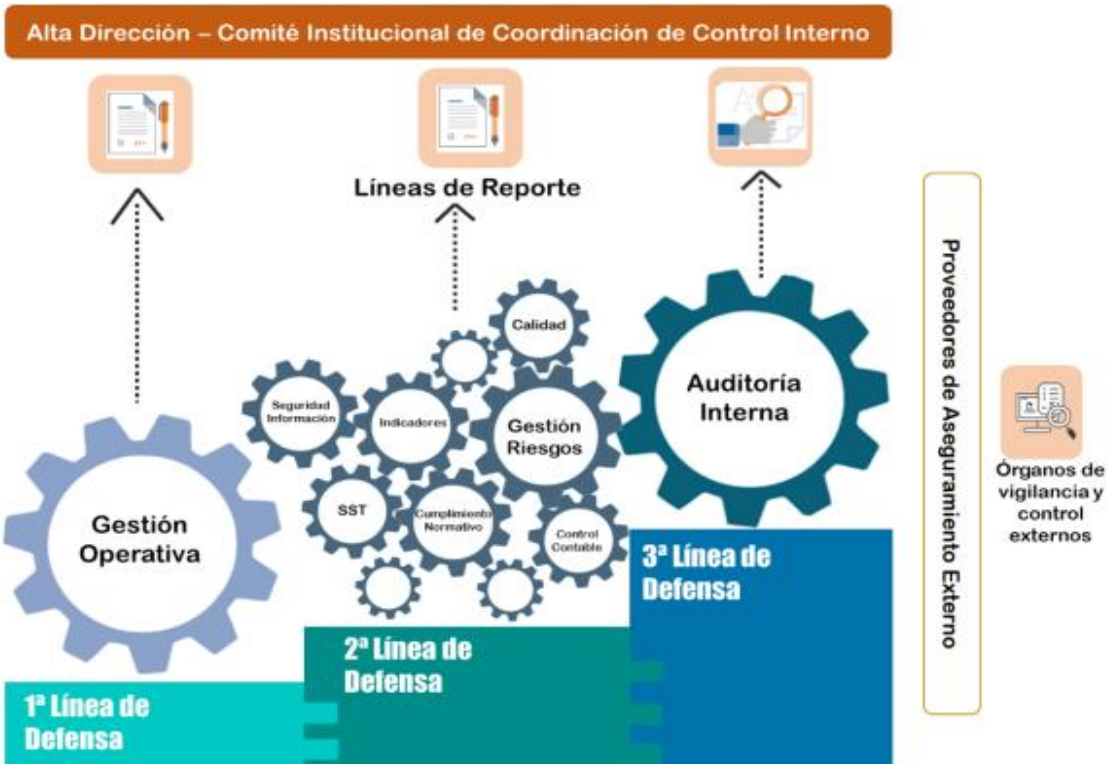
El responsable de la seguridad digital adicionalmente deberá:

Definir y actualizar cuando sea necesario el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de Riesgo de seguridad digital.

- Definir y actualizar cuando sea necesario el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Establecer un documento con la declaración de aplicabilidad de los controles del Anexo A de la ISO/IEC 27001:2013
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.

- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.



Fuente: Manual Operativo MIPG. Gráfico 18. Versión 5 - marzo de 2023.

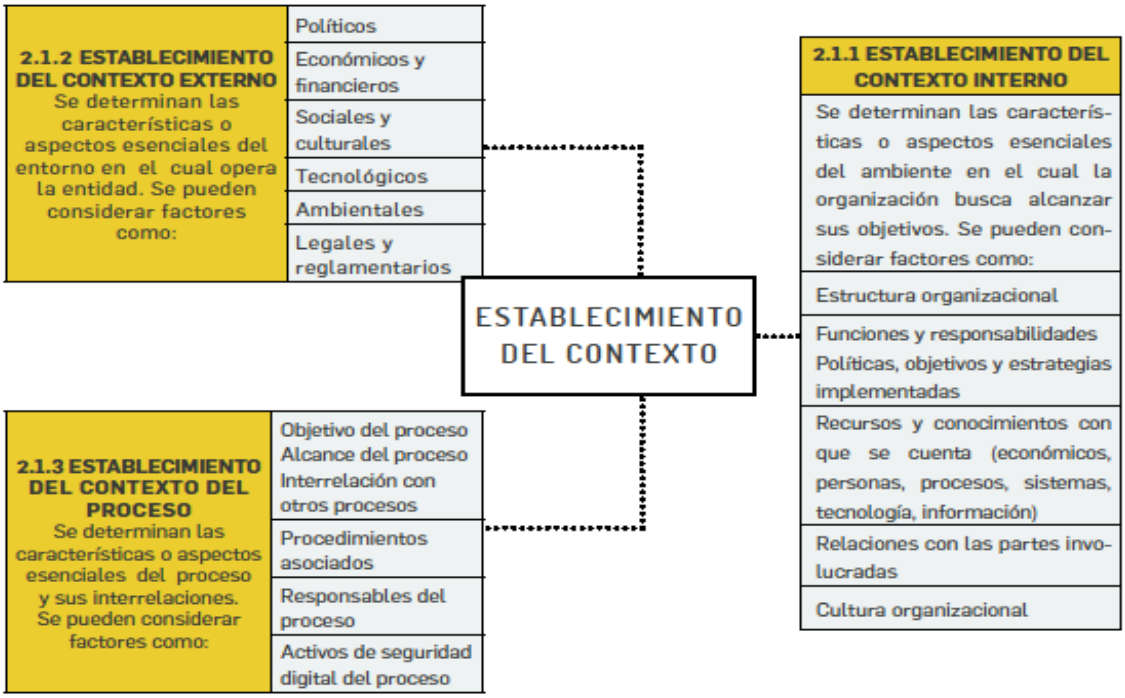
8. METODOLOGÍA A UTILIZAR

La metodología a implementar en el Cuerpo Oficial de Bomberos de Dosquebradas se realizará de acuerdo a la guía de riesgos de la Función Pública vigente. Para los riesgos de Corrupción de acuerdo a los lineamientos dados por la Secretaría de Transparencia de la Presidencia de la República que se encuentran establecidos en la Guía de Gestión del Riesgo de Función Pública versión No.4 de 2018.

9. ESTABLECIMIENTO DEL CONTEXTO

Se tienen definidos los objetivos institucionales que deben desarrollar a través de sus diferentes planes, programas y proyectos. Su cumplimiento puede verse afectado por la presencia de riesgos, es decir por la probabilidad de ocurrencia de hechos o actos, producto de factores internos, externos o de procesos que obstaculizan el normal desarrollo de las funciones, siendo en este punto, en donde es necesario contar con una herramienta para su administración.

En esta fase, se debe analizar contexto externo, contexto interno, contexto del proceso y activos de seguridad digital, analizando los siguientes elementos:



Ejemplos de Factores de Riesgo:

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)

Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Frente a los riesgos de seguridad digital y previo a su identificación se deben identificar los activos de información siguiendo estos pasos:

- Listar los activos por cada proceso: En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

- Identificar el dueño de los activos: Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.
- Clasificar los activos: Cada activo debe tener una clasificación o pertenecer a un determinado grupo según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros.
- Clasificar la información: Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información.
- Determinar la criticidad del activo: La entidad pública debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado adecuado de cada caso. importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.
- Identificar si existe infraestructura crítica cibernética: Se invita a que las entidades públicas identifiquen y reporten a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios: impacto social, impacto económico e impacto ambiental.

10. IDENTIFICACIÓN DEL RIESGO

Para la identificación de los riesgos es fundamental la definición de los Objetivos de los procesos:

Objetivos de Procesos: Son los resultados que se esperan lograr para cumplir la misión y visión de la entidad. Determina el cómo la política trazada y el aporte que se hace a los objetivos institucionales.

Un objetivo es un enunciado que expresa una acción, por lo tanto, debe iniciarse con un verbo fuerte como: Establecer, Identificar, recopilar, investigar, registrar buscar, así mismo se debe tratar que contenga la estructura del: Qué, Cómo y el para qué. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción

10.1 RIESGO DE GESTIÓN:

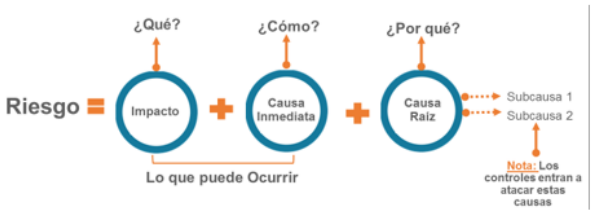
La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno y externo y del proceso que pueden afectar el logro de los objetivos. Es importante analizar aquellos eventos o situaciones que pueden afectar el normal desarrollo de los objetivos del proceso u objetivos estratégicos. Preguntas a tener en cuenta (Qué puede suceder, como

puede suceder, por qué puede suceder). Es importante tener en cuenta la siguiente grafica para la identificación de los Riesgos de Gestión:

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Ejemplo aplicado

Proceso: Gestión de Recursos:
Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación



Redacción inicia con: ¿Qué? ¿Cómo?

Posibilidad de afectación reputacional sanción del ente de control, debido a adquisición de bienes y servicios fuera de los requerimientos normativos.

¿Por qué?

10.2 RIESGOS DE CORRUPCIÓN:

Los riesgos de corrupción se establecen sobre procesos. 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.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, 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: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

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

Ejemplo de redacción de Riesgo de Corrupción: Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros para favorecer a un proponente con una adjudicación.

10.3 RIESGOS DE SEGURIDAD DIGITAL:

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o grupo de activos dentro del proceso. “integridad, confidencialidad o disponibilidad”. Para el riesgo de este tipo se debe asociar el grupo de activos o activos específicos del proceso y analizar amenazas o vulnerabilidades que podrían causar su materialización.

En este sentido existirán tres tipos de riesgos: Pérdida de confidencialidad, pérdida de integridad y pérdida de disponibilidad de los activos. Para cada riesgo se debe asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto es necesario consultar el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:

Tabla 5. Tabla de amenazas comunes
Tabla 6. Tabla de amenazas dirigida por el hombre

Tabla 7. Tabla de vulnerabilidades comunes

Ejemplo de Riesgo de Seguridad Digital:

Fuga o acceso de información por personal no autorizado

Descripción del Riesgo:

La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.

11. VALORACIÓN DE RIESGOS

La valoración de los riesgos consiste en analizar las causas, establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE)

11.1 CÁLCULO DE LA PROBABILIDAD RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL:

Determinar la probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, 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.

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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

11.2 CÁLCULO DE LA PROBABILIDAD RIESGOS DE CORRUPCIÓN:

Se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

NIVEL	DESCRIPTOR	DESCRIPCION	FRECUENCIA

1	**Raro**	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	**Improbable**	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
3	**Posible**	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	**Probable**	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez en el último año
5	**Casi Seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

11.3 ANÁLISIS DEL IMPACTO RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL:

Determinar el impacto: Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferente niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico menor 40% (entre 10 y 50 SMLMV) y un impacto reputacional mayor 80% (el riesgos afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel Departamental o Municipal) en este ejemplo para el impacto se tomará el más alto xx (el reputacional) es decir que se establece un impacto mayor correspondiente al 80%.

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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

11.4 ANÁLISIS DEL IMPACTO RIESGOS DE CORRUPCIÓN:

Tabla 5. Criterios para calificar el impacto - riesgos de corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
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.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

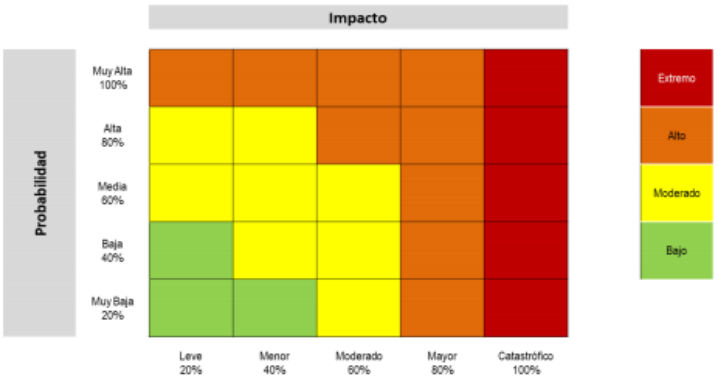
Nivel de impacto MAYOR

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

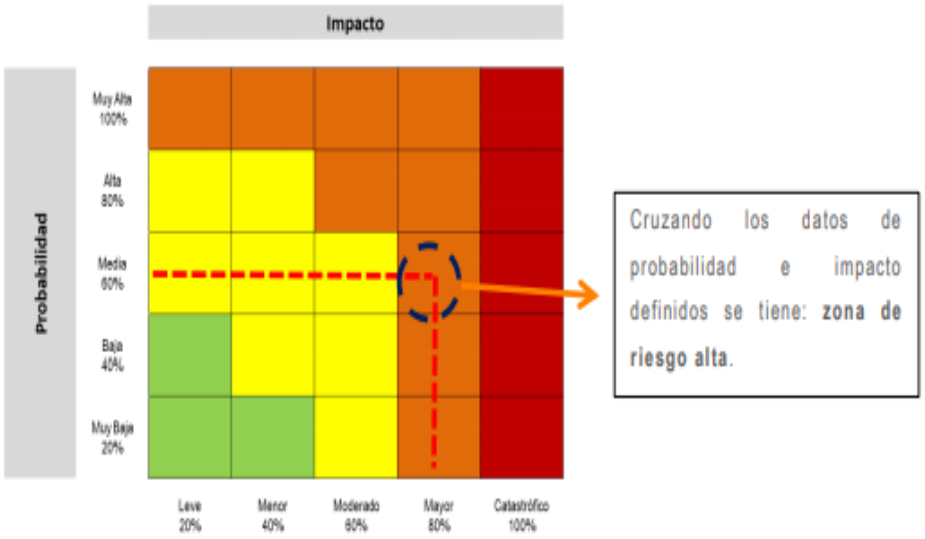
12. EVALUACIÓN DE RIESGOS

12.1 ANÁLISIS PRELIMINAR: MAPA DE CALOR PARA, RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL (RIESGO INHERENTE).

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

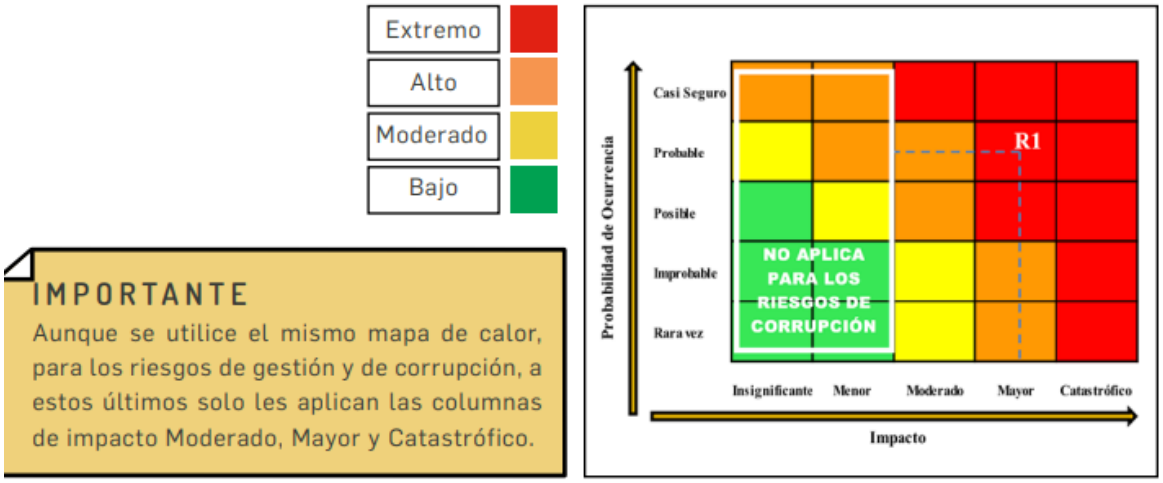


Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.



12.2 ANÁLISIS PRELIMINAR: MAPA DE CALOR PARA, RIESGOS DE CORRUPCIÓN (RIESGO INHERENTE)

Se toma la calificación de probabilidad y la calificación de impacto, ubicando la probabilidad en la fila y el impacto en las columnas correspondientes, posterior establezca el punto de intersección de las dos y este punto corresponderá al nivel de riesgo.



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

NOTA: FRENTE A LOS RIESGOS DE CORRUPCIÓN <u>NO APLICAN LOS NIVELES DE IMPACTO INSIGNIFICANTE Y MENOR.</u>

13. DISEÑO Y VALORACIÓN DE CONTROLES RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL

Valoración de controles: en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

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

13.1 ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL

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

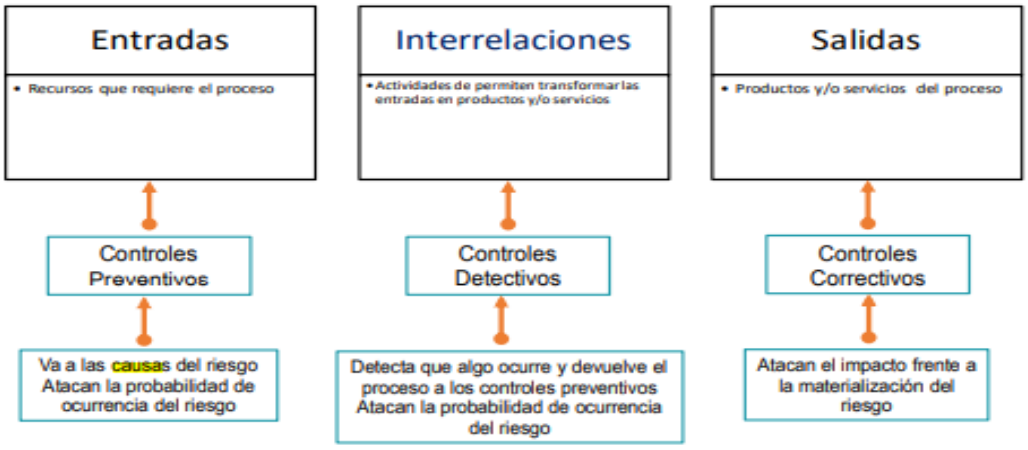
- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

13.2 TIPOS DE CONTROLES

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

NOTA: Para los riesgos de corrupción, solo aplican controles detectivos y preventivos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- Control manual: controles que son ejecutados por personas.
- Control automático: son ejecutados por un sistema.

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%
	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%
*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.	-
		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.	-

13.3 CONTROLES ASOCIADOS A SEGURIDAD DIGITAL

El Cuerpo Oficial de Bomberos de Dosquebradas, podrá mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, 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.

13.4 IDENTIFICACIÓN DE LOS CONTROLES EXISTENTES EN SEGURIDAD DIGITAL

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

Los controles que se planifican para implementar de acuerdo con los planes de implementación de tratamiento de riesgo se deberían considerar en la misma forma que aquellos que ya están implementados.

Un control existente planificado se podría calificar como ineficaz, insuficiente o injustificado, si es injustificado o insuficiente, se debería revisar el control para determinar si se debe eliminar o reemplazar por otro más adecuado.

Actividades para revisar controles existentes o planificados:

- Revisando los documentos que contengan información sobre los controles.
- Verificación con las personas responsables de la seguridad de la información y los usuarios.
- Efectuar revisiones en sitio comparando los controles implementados contra la lista de controles que deberían estar.
- Cuáles están implementados correctamente y si son o no eficaces.
- Revisión de los resultados de las auditorías internas.

13.5 DISEÑO Y VALORACIÓN DE CONTROLES RIESGOS DE CORRUPCIÓN

Valoración de controles y diseño de controles: Al momento de definir un control se debe tener en cuenta desde la redacción las siguientes variables:

Análisis y evaluación de los controles y peso en la evaluación del diseño del control para Riesgos de Corrupción.

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	15 Asignado	0 No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	15 Adecuado	0 Inadecuado
2. Periodicidad	¿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?	15 Oportuna	0 Inoportuna
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.?	15 Prevenir o detectar 10	0 No es un control
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?.	15 Confiable	0 No confiable
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	15 Se investigan y resuelven oportunamente	0 No se investigan y resuelven oportunamente.
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?.	10 Completa	5 Incompleta / no existe 0

Resultados de la evaluación del diseño de control

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO – PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Nota:

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

La evaluación de los riesgos se realiza antes y después de los controles. Es importante garantizar que los controles estén bien diseñados teniendo en cuenta los siguientes elementos:

- Para cada causa debe existir un control.
- Las causas se deben trabajar de manera separada.
- Un control puede ayudar a mitigar varias causas, en estos casos se repite el control asociado de manera independiente a la causa específica.

Resultados de la evaluación de la ejecución del control

En esta parte de la matriz se evalúa no solo que el control este bien diseñado, se debe asegurar que el control se ejecute correctamente. En primera instancia el responsable del proceso debe confirmar, posteriormente se confirma con las actividades de evaluación realizadas por auditorías internas o control interno.

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO - PESO DE LA EJECUCIÓN DEL CONTROL -
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

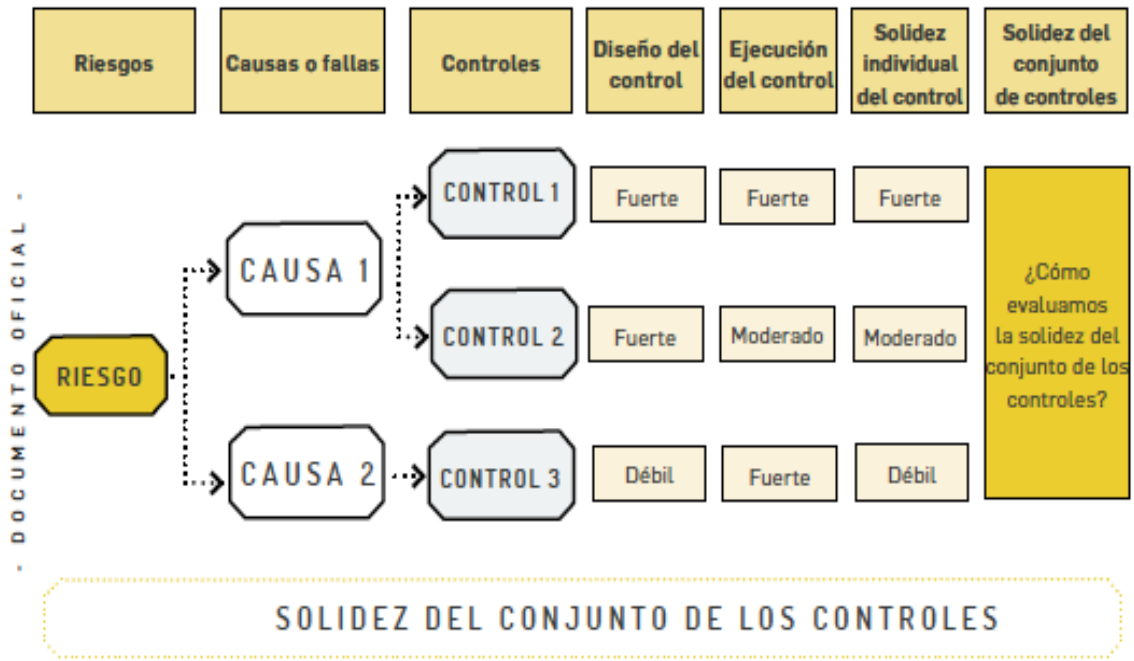
Análisis y evaluación de controles para mitigación de los riesgos:

Mediante la siguiente calificación se analiza la solidez del control en cuanto a su diseño y en cuanto a su ejecución, finalmente se identifica la solidez del control y se define de acuerdo a dicha valoración si es necesario establecer acciones para fortalecer el control. Siguiendo siguiente metodología:

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	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Finalmente, la solidez del conjunto de controles para una adecuada mitigación del riesgo se califica de la siguiente manera:

Esquema 12. Solidez del conjunto de controles

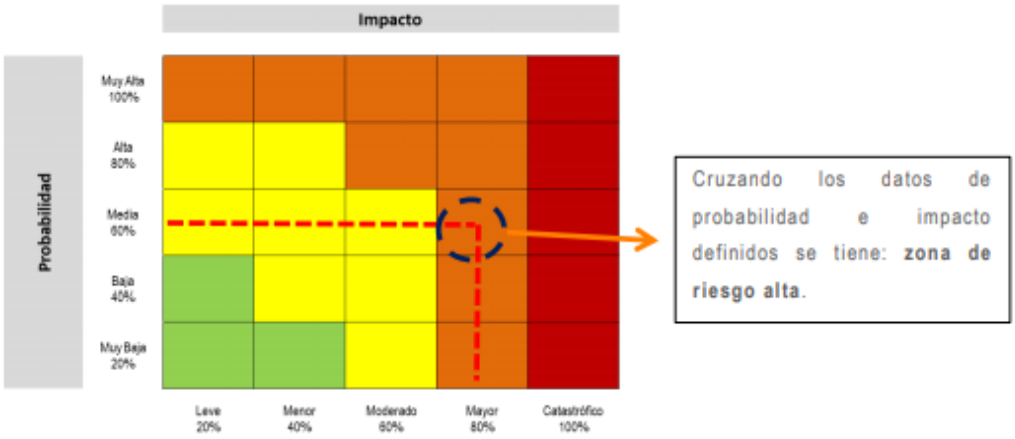


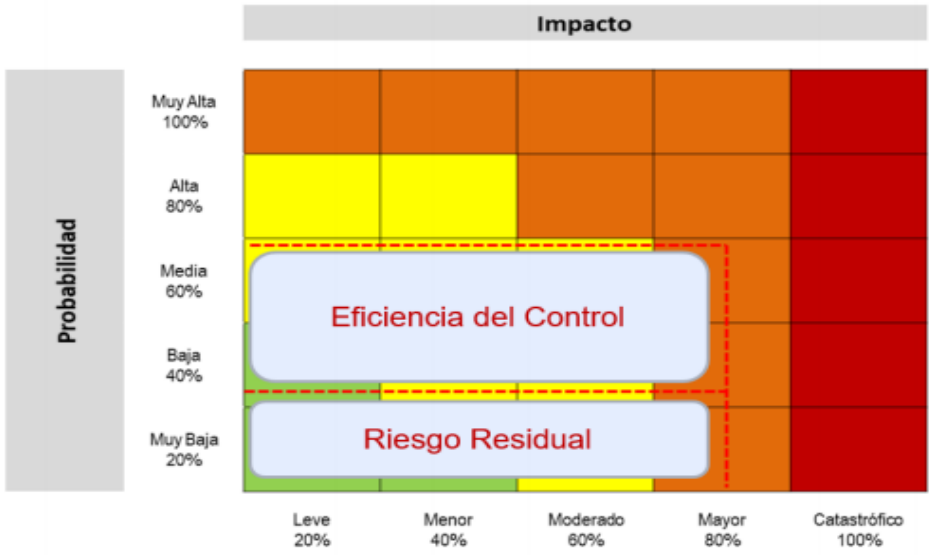
IMPORTANTE
La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

14. NIVEL DE RIESGO (RIESGO RESIDUAL) PARA LOS RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL:

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

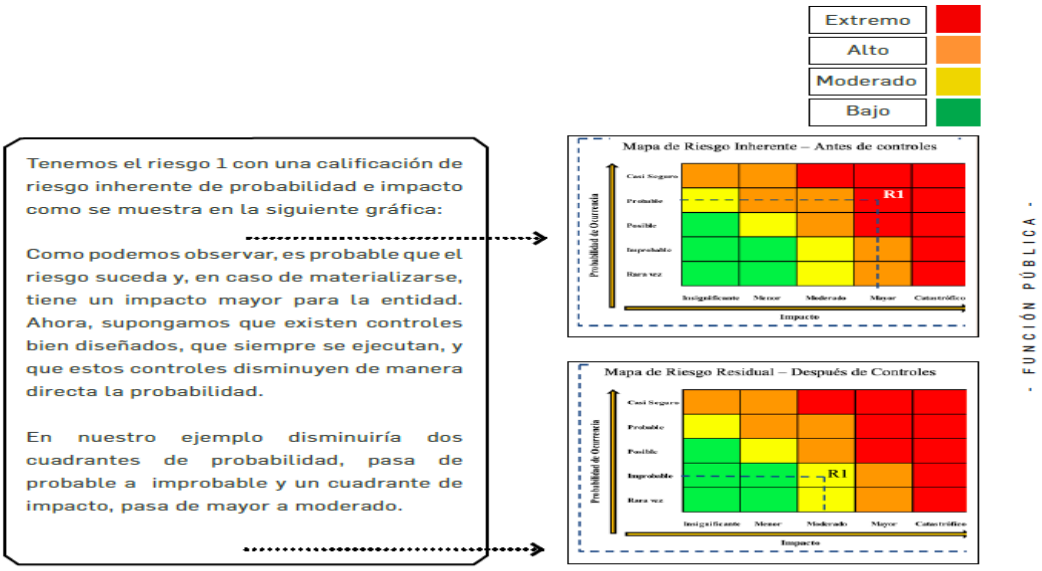




Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

14.1 RESULTADOS DEL MAPA DE RIESGOS RESIDUAL RIESGOS DE CORRUPCIÓN

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).



15. ESTRATEGIAS PARA COMBATIR EL RIESGO DE GESTIÓN Y SEGURIDAD DIGITAL

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente. En la siguiente figura se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos:

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

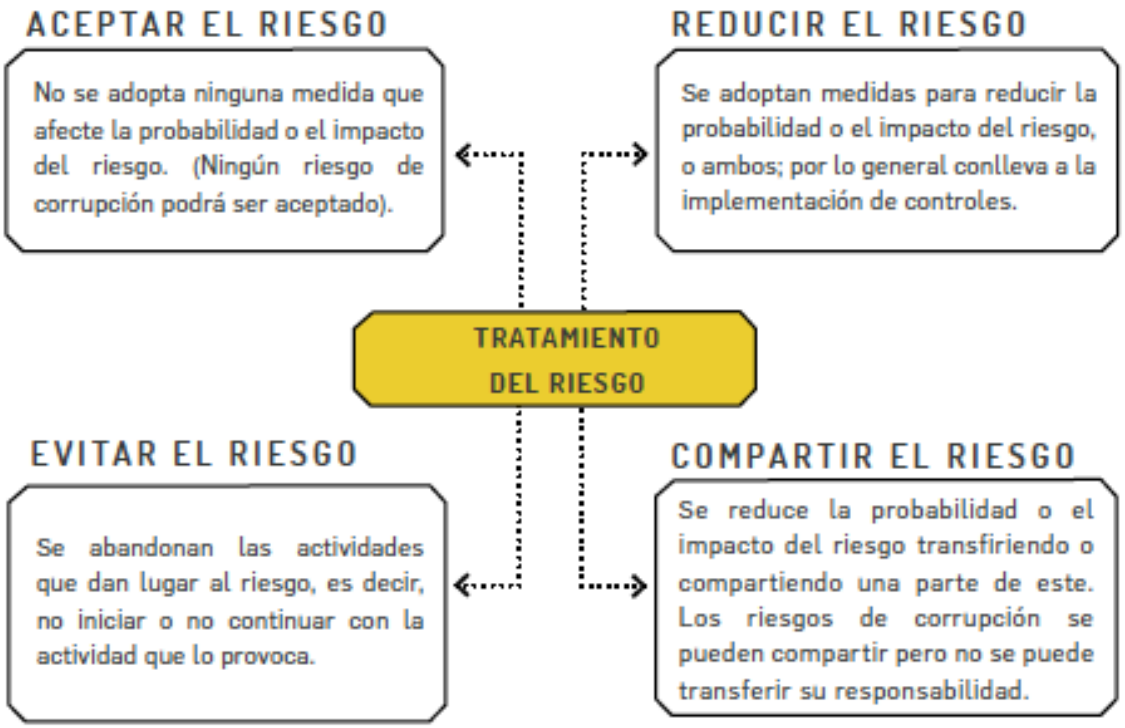
Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique:

- Responsable,
- Fecha de implementación,
- Fecha de seguimiento.

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca dentro del Plan de Continuidad de Negocio 2 y se consideraría un control correctivo.

Nota: Para mitigar / tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001:2013 “Lineamientos para la gestión del riesgo de seguridad digital”, lineamientos que hacen parte integral de la presente política.

15.1 TRATAMIENTO DEL RIESGO DE CORRUPCIÓN (OPCIONES DE MANEJO):



Ningún Riesgo de Corrupción se Acepta ni se transfiere su responsabilidad

16. MONITOREO Y REVISIÓN A RIESGOS DE CONTRATACIÓN, RIESGOS DE CORRUPCIÓN, RIESGOS DE GESTIÓN, RIESGOS DE SEGURIDAD DIGITAL, RIESGOS DE SST

El monitoreo y revisión de los riesgos está alineado a la dimensión de control interno del MIPG, el cual se encuentra establecido a través de asignación de responsabilidades y roles en el marco de las líneas de defensa.

Riesgos de gestión, riesgos de corrupción y riesgos de seguridad digital son monitoreados de manera permanente por los líderes de proceso y sus equipos de trabajo, dichos monitoreos y revisiones se realizan y se formalizan de manera trimestral y semestral siguiendo la siguiente frecuencia. En el caso de los riesgos de seguridad digital, se debe reportar en el mapa y planes de tratamiento. El responsable de seguridad digital apoyará y acompañará a las diferentes líneas de defensa tanto para el reporte, como para la gestión y el tratamiento de estos riesgos.

El Cuerpo Oficial de Bomberos de Dosquebradas a través de las Tres Líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, Componente Actividades de control, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación: Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Nota: una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad pública debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

16.1 SEGUIMIENTO RIESGOS EN EL PROCESO DE CONTRATACIÓN

a. En la etapa de planeación contractual: Corresponde al Ordenador del Gasto, a los Directores Operativos, Administrativos, Jefes de Oficina.

b. En la etapa de ejecución contractual: Corresponde a los Supervisores Contractuales.

Seguimiento Etapa de Planeación: Antes de remitir la solicitud de inicio de proceso de contratación al área Jurídica. (como evidencia el aval de la matriz de Riesgos de Contratación).

Seguimiento Etapa de Ejecución Contractual: Se entiende realizado con la suscripción por parte del Supervisor de las actas parciales o finales. El tratamiento se realizará de acuerdo al tipo de riesgo y a la etapa en la cual se encuentre el contrato.

16.2 FECHAS DE REPORTE POR PARTE DE LÍDERES DE PROCESO / EQUIPOS DE TRABAJO RIESGOS CORRUPCIÓN:

- 1er reporte periodo (enero – febrero – marzo): el plazo de reporte deberá surtirse dentro de los diez (10) primeros días calendario del mes de abril.
- 2do reporte periodo (abril – mayo – junio): El plazo de reporte deberá surtirse dentro de los diez (10) primeros días calendario del mes de julio.

- 3ro reporte periodo (julio – agosto – septiembre): el plazo de reporte deberá surtirse dentro de los diez (10) primeros días calendario del mes de octubre.
- 4to reporte periodo (octubre – noviembre – diciembre): el plazo de reporte deberá surtirse la última semana del mes de diciembre.

16.3 FECHAS DE REPORTE POR PARTE DE LÍDERES DE PROCESO / EQUIPOS DE TRABAJO RIESGOS DE GESTIÓN:

- 1er reporte periodo (diciembre -enero -febrero -marzo - abril - mayo): Plazo de reporte deberá surtirse dentro de los diez (10) primeros días calendario del mes de junio.

- 2do reporte periodo (junio - julio - agosto - septiembre - octubre - noviembre): el plazo de reporte deberá surtirse dentro de los diez (10) primeros días calendario del mes de diciembre.

16.4 FECHA DE MONITOREO RIESGOS DE CORRUPCIÓN POR PARTE DE LA SUBGERENCIA ADMINISTRATIVA Y FINANCIERA:

El área de Direccionamiento y Planeación en cabeza de la Subgerente Administrativa y Financiera realizará de manera trimestral el monitoreo al PAAC en el cual está inmerso el informe de los riesgos de Corrupción.

- 1er reporte periodo (enero – febrero – marzo): el plazo de reporte deberá surtirse dentro de los veinte (20) primeros días hábiles del mes de abril.
- 2do reporte periodo (abril – mayo – junio): El plazo de reporte deberá surtirse dentro de los veinte (20) primeros días hábiles del mes de julio.
- 3ro reporte periodo (julio – agosto – septiembre): el plazo de reporte deberá surtirse dentro de los veinte (20) primeros días hábiles del mes de octubre.
- 4to reporte periodo (octubre – noviembre – diciembre): el plazo de reporte deberá surtirse dentro de los veinte (20) primeros días hábiles del mes de enero.

16.5 FECHA DE MONITOREO RIESGOS DE GESTIÓN POR PARTE DE LA SUBGERENCIA ADMINISTRATIVA Y FINANCIERA

- 1er reporte periodo (diciembre -enero -febrero -marzo - abril - mayo): Plazo de reporte deberá surtirse dentro de los veinte (20) días hábiles del mes de junio.

- 2do reporte periodo (junio - julio - agosto - septiembre - octubre - noviembre): el plazo de reporte deberá surtirse dentro de los veinte (20) días hábiles del mes de diciembre.

16.6 REGISTRO Y REPORTE DE INCIDENTES DE SEGURIDAD DIGITAL:

Es importante que la entidad pública cuente con el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

16.7 REPORTE DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL AL INTERIOR DE LA ENTIDAD

El responsable de seguridad digital debería reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

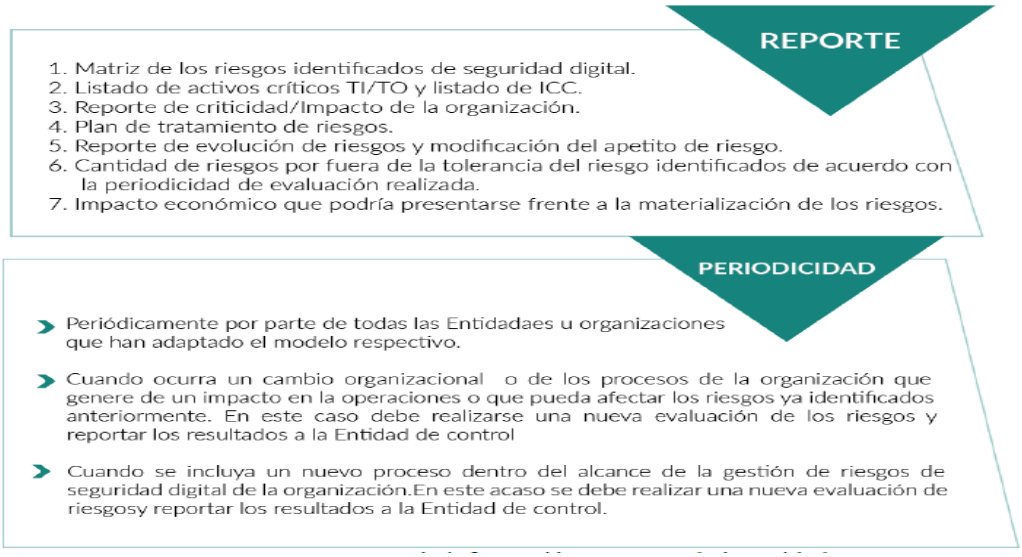


Imagen 3. Reportes de información por parte de la entidad.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Igualmente, en el caso de los riesgos de seguridad digital, se debe reportar en el mapa y planes de tratamiento. Se deben generar indicadores, para medir la gestión realizada, en esencia en cuanto a la eficacia y la efectividad de los planes de tratamiento implementados.

La entidad deberá preferiblemente definir como mínimo 2 indicadores POR PROCESO de la siguiente manera:

- Indicador de eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.
- Indicador efectividad, para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, e integridad, de disponibilidad).

16.8 SEGUIMIENTO RIESGOS DE SST:

El área de Talento Humano, a través de Seguridad y Salud en el Trabajo, realizará el seguimiento a la Matriz de riesgos de SST de acuerdo con lo definido en sus procedimientos e instructivos internos.

16.9 SEGUIMIENTO POR CONTROL INTERNO A RIESGOS DE GESTIÓN:

El seguimiento realizado a los Riesgos de Gestión será efectuado una vez al año y programado en el plan de acción de cada vigencia de la Oficina Asesora de Control Interno.

16.10 ACTIVIDADES A ADELANTAR PARA EL SEGUIMIENTO A LOS RIESGOS POR PARTE DE CONTROL INTERNO.

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.

Se adoptan las fechas y parámetros establecidos para el seguimiento a los riesgos de corrupción inmerso en el seguimiento al Plan Anticorrupción y Atención al Ciudadano de la siguiente manera:

- **Primer seguimiento:** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.
- **Segundo seguimiento:** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre.
- **Tercer seguimiento:** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

16.11 PARA LOS SEGUIMIENTOS DE CONTROL INTERNO A LOS RIESGOS SE DEBERÁ ADELANTAR LAS SIGUIENTES ACTIVIDADES:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión aleatoria de los riesgos de Gestión y Corrupción y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

- Harán parte de la política de administración del riesgo los resultados de las evaluaciones llevadas a cabo por los diferentes órganos de control, los cuales reposarán en la oficina Asesora de Control Interno siendo un insumo para la identificación y tratamiento de los diferentes riesgos.

17. 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:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción.
- Realizar un monitoreo permanente.

Teniendo en cuenta que la Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva. Las acciones adelantadas se refieren a:

- Acciones encaminadas a determinar la efectividad de los controles.
- Acciones encaminadas a mejorar la valoración de los riesgos.
- Acciones encaminadas a mejorar los controles.
- Analizar el diseño e idoneidad de los controles, si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

18. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DE RIESGOS DE GESTIÓN

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

- Acciones encaminadas a determinar la efectividad de los controles.
- Acciones encaminadas a mejorar la valoración de los riesgos.
- Acciones encaminadas a mejorar los controles.
- Analizar el diseño e idoneidad de los controles, si son adecuados para prevenir o mitigar los riesgos de gestión
- Elaboración de plan de mejoramiento en el cual se deben registrar acciones encaminadas en el fortalecimiento de los controles del riesgo que se materializó
- valoración de la probabilidad e impacto del riesgo materializado

19. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas, tanto internas como externas debe tener lugar durante todas las etapas del proceso para la gestión del riesgo.
Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.
La comunicación y consulta se constituye en un elemento transversal a todo el proceso al involucrar a todos los funcionarios para el levantamiento de los mapas de riesgos, con el fin de ayudar a establecer correctamente el contexto para los procesos, garantizar que se toman en consideración las necesidades de los usuarios, ayudar a garantizar que los riesgos estén correctamente identificados, reunir diferentes áreas de experticia para el análisis de los riesgos, garantizar que los diferentes puntos de vista se toman en consideración adecuadamente durante todo el proceso, fomentar la administración del riesgo como una actividad inherente al proceso de planeación estratégica.

20. RIESGOS EN EL PROCESO DE CONTRATACIÓN

20.1 INTRODUCCIÓN:

La regulación normativa de los riesgos en la contratación pública no es muy amplia, a saber: Ley 1150 de 2007, Decreto 1082 de 2015 y los documentos Conpes, que conforman el conjunto normativo y reglamentario relacionado con la gestión de los riesgos en la contratación pública.

Es necesario tener en cuenta el principio de planeación, en la medida que un adecuado análisis y evaluación de riesgos en la etapa precontractual basado en estudios técnicos y científicos, permiten identificar y anticipar los eventos futuros adversos a los intereses perseguidos con la contratación, identificar las causas, sus efectos y los resultados que pueden producirse.

El Decreto 1082 de 2015, definió el riesgo como aquel «evento que puede generar efectos adversos y de distinta magnitud en el logro de los objetivos del Proceso de Contratación o en la ejecución de un Contrato» (art. 2.2.1.1.1.3.1).

A su vez, estableció el deber de análisis de riesgo durante la etapa de planeación para conocer el sector relativo al objeto del proceso de contratación (art. 2.2.1.1.1.6.1) y evaluar el riesgo que el proceso de contratación representa para el cumplimiento de sus metas y objetivos (art. 2.2.1.1.1.6.3).

Además, establece que para los procesos de selección que sean adelantados bajo la modalidad de licitación pública, deberá darse una audiencia para la asignación de riesgos, en donde la entidad deberá presentar el análisis de estos y realizar su asignación definitiva (art. 2.2.1.2.1.1.2).

Esta reglamentación se consolidó en el Decreto 1082 de 2015, en la que se determinaron los riesgos que deben cubrir las garantías en la contratación pública, en cuanto al cumplimiento de las obligaciones surgidas en favor del Estado con ocasión de «(i) la presentación de las ofertas; (ii) los contratos y su liquidación; y (iii) los riesgos a los que se encuentran expuestas las Entidades Estatales, derivados de la responsabilidad extracontractual que pueda surgir por las actuaciones, hechos u omisiones de sus contratistas y subcontratistas, deben estar garantizadas en los términos de la ley y del presente título» (art. 2.2.1.2.3.1.1)

Los lineamientos emitidos por el Conpes, dentro de los cuales cabe destacar el documento 3107 de 2001, en el cual se fijaron los lineamientos de la «Política de manejo de riesgo contractual del Estado para procesos de participación privada en infraestructura» en los sectores de transporte, energía, comunicaciones y agua.

El documento Conpes 3714 de 2011, el cual desarrolló los lineamientos básicos para entender el concepto de riesgo previsible en el marco de las adquisiciones sometidas al Estatuto General de Contratación de la Administración Pública, con el propósito de fortalecer y unificar los procedimientos de la etapa precontractual para la tipificación, estimación y asignación de riesgos previsibles de la contratación pública.

En la etapa poscontractual se encuentran los mecanismos de cobertura del riesgo que son las garantías, las cuales tienen como objeto resarcir el detrimento patrimonial que se ocasiona, ya sea por incumplimiento de las obligaciones del contratista, inadecuada gestión fiscal del servidor público encargado, pérdida o deterioro del bien o por eventos que comprometen la responsabilidad patrimonial del Estado frente a terceros.

No obstante, para algunas circunstancias acaecidas durante la ejecución que tienen el carácter de imprevisible y que afectaron la ecuación financiera del contrato, en muchas ocasiones puede que no se encuentren estas contingencias dentro de la cobertura de las garantías.

Para tal fin, como forma adecuada de administración o gestión de los riesgos, las entidades públicas cuentan con la etapa de la liquidación del contrato, escenario adecuado para realizar un balance económico, jurídico y técnico de lo ejecutado, así como para determinar los hechos o circunstancias que afectaron la ejecución normal del negocio y establecer el estado en que las partes quedan frente a este.
Los Tipos de Riesgos, establecidos son los siguientes:
PREVISIBLES: el documento Conpes 3714 de 2011, Son "todas aquellas circunstancias que, de presentarse durante el desarrollo y ejecución del contrato, tienen la potencialidad de alterar el equilibrio financiero del mismo, siempre que sean identificables y cuantificables en condiciones normales".
IMPREVISIBLES «tanto los anormales que no fueron previstos en el contrato, como también los que habiéndolo sido, sus efectos desbordan los límites de la asunción de la parte contratante a quien dichos riesgos le fueron distribuidos», tienen especial importancia, si se tiene en cuenta que al tratarse de situaciones no previstas al momento de celebrar el contrato o que desbordan el deber que tiene el contratista de soportarlas, dan lugar, al contratista, para alegar el rompimiento de la ecuación contractual, y por tanto, solicitar a la administración el restablecimiento económico del mismo.

RIESGO CONTRACTUAL: Es la medida de la variabilidad de los posibles resultados que se pueden esperar de un evento. Aquellas circunstancias que pueden presentarse durante el desarrollo o ejecución de un contrato y que pueden alterar el equilibrio financiero del mismo y ha tenido una regulación desde cinco (5) ópticas, asociadas con el proceso de gestión que se requiere en cada caso, las cuales son las siguientes: Riesgos Previsibles, Riesgos Imprevisibles, Riesgos Cubiertos por el Régimen de Garantías, Obligaciones Contingentes, Riesgos Generados por Malas Prácticas.

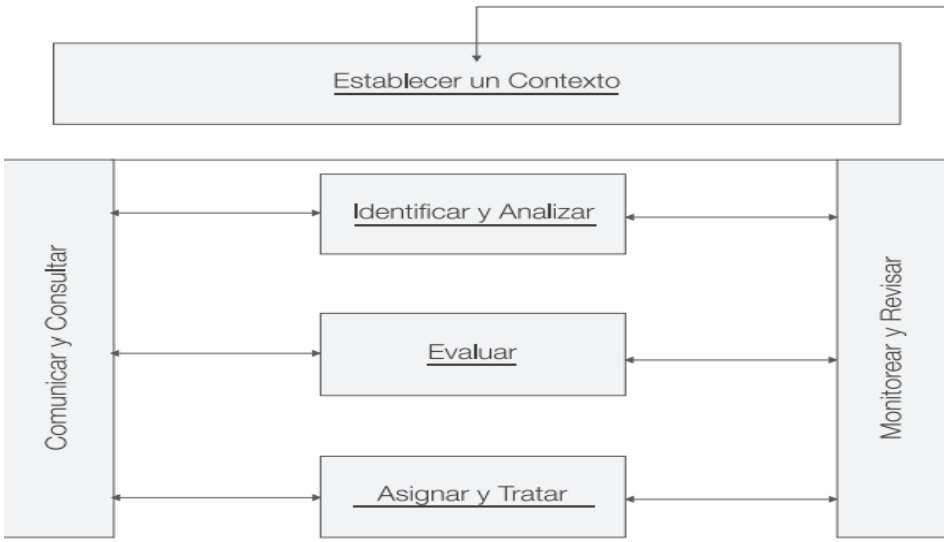
20. 2 ESTRUCTURA DE LA ADMINISTRACIÓN DE RIESGOS CONTRATACIÓN

De acuerdo con lo establecido por la Agencia Colombia Compra Eficiente en su Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación:

1. La administración o el manejo del riesgo debe cubrir desde la planeación hasta la terminación del plazo, la liquidación del contrato, el vencimiento de las garantías de calidad o la disposición final del bien; y no solamente la tipificación, estimación y asignación del riesgo que pueda alterar el equilibrio económico del contrato.

2. Se debe estructurar un sistema de administración de Riesgos teniendo en cuenta, entre otros, los siguientes aspectos: (a) los eventos que impidan la adjudicación y firma del contrato como resultado del Proceso de Contratación; (b) los eventos que alteren la ejecución del contrato; (c) el equilibrio económico del contrato; (d) la eficacia del Proceso de Contratación, es decir, que la Entidad Estatal pueda satisfacer la necesidad que motivó el Proceso de Contratación; y la reputación y legitimidad de la Entidad Estatal encargada de prestar el bien o servicio.

3. Colombia Compra Eficiente propone administrar los Riesgos del Proceso de Contratación como se establece a continuación:



20.3 CONTEXTO

La Alcaldía debe tener conocimiento del ambiente social, económico y político, que le rodea y, en consecuencia, debe identificar:

(i) Sus propios Riesgos;
(ii) los Riesgos comunes a sus Procesos de Contratación; y
(iii) los Riesgos del Proceso de Contratación en particular.

20.4 IDENTIFICAR Y CLASIFICAR LOS RIESGOS

Para ello se debe diligenciar la siguiente Matriz propuesta por la Agencia Colombia Compra Eficiente: en sus ítems:

N	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le asigna?	Tratamiento/Control a ser implementado	Impacto después del tratamiento				¿Afecta la ejecución del contrato?	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría	Responsable por implementar el tratamiento			¿Cómo se realiza el monitoreo?	Periodicidad
[Numerar consecutivamente empezando en 1]	[General/Específico]	[Interno/Externo]	[Planeación/Selección/Contratación/Ejecución]	[Económico/ Social o político/ Operacional/ Financiero/ Regulatorio/ De la naturaleza/ Ambiental/ Tecnológico]	[Describir el Riesgo]	[Describir la consecuencia de la ocurrencia del evento]	[1/2/3/4/5]	[1/2/3/4/5]	[2/3/4/5/6/7/8/9/10]	[Bajo/Medio/Alto/Extremo]	[Entidad Estatal/Contratista]	[Describir el tratamiento o control a ser implementado]	[1/2/3/4/5]	[1/2/3/4/5]	[2/3/4/5/6/7/8/9/10]	[Bajo/Medio/Alto/Extremo]	[SI/No]	[Entidad Estatal/Contratista]	[Incluir fecha o evento con el cual se inicia el tratamiento]	[Incluir fecha o evento con el cual se inicia el tratamiento]	[Definir la forma de realizar el monitoreo]	[Definir la periodicidad del monitoreo]

20.5 EVALUAR Y CALIFICAR LOS RIESGOS

Se debe evaluar cada uno de los Riesgos identificados, estableciendo el impacto de los mismos frente al logro de los objetivos del Proceso de Contratación y su probabilidad de ocurrencia.

a. Probabilidad

	Categoría	Valoración
Probabilidad	Raro (puede ocurrir excepcionalmente)	1
	Improbable (puede ocurrir ocasionalmente)	2
	Posible (puede ocurrir en cualquier momento futuro)	3
	Probable (probablemente va a ocurrir)	4
	Casi cierto (ocurre en la mayoría de circunstancias)	5

b. Impacto del Riesgo

Impacto						
Calificación Cualitativa		Obstruye la ejecución del contrato de manera intrascendente.	Dificulta la ejecución del contrato de manera baja. Aplicando medidas mínimas se puede lograr el objeto contractual.	Afecta la ejecución del contrato sin alterar el beneficio para las partes.	Obstruye la ejecución del contrato sustancialmente pero aun así permite la consecución del objeto contractual.	Perturba la ejecución del contrato de manera grave imposibiltando la consecución del objeto contractual.
Calificación Monetaria		Los sobrecostos no representan más del uno por ciento (1%) del valor del contrato.	Los sobrecostos no representan más del cinco por ciento (5%) del valor del contrato.	Genera un impacto sobre el valor del contrato entre el cinco (5%) y el quince por ciento (15%).	Incrementa el valor del contrato entre el quince (15%) y el treinta por ciento (30%).	Impacto sobre el valor del contrato en más del treinta por ciento (30%).
Categoría	Valoración	Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5

c. Valoración del Riesgo:

Para ello se debe proceder a sumar las valoraciones de probabilidad e impacto, para obtener la valoración total del Riesgo:

			Impacto				
	Calificación Cualitativa		Obstruye la ejecución del contrato de manera intrascendente.	Dificulta la ejecución del contrato de manera baja, aplicando medidas mínimas se pueden lograr el objeto contractual.	Afecta la ejecución del contrato sin alterar el beneficio para las partes.	Obstruye la ejecución del contrato sustancialmente pero aun así permite la consecución del objeto contractual.	Perturba la ejecución del contrato de manera grave imposibilitando la consecución del objeto contractual.
	Calificación Monetaria		Los sobrecostos no representan más del uno por ciento (1%) del valor del contrato.	Los sobrecostos no representan más del cinco por ciento (5%) del valor del contrato.	Genera un impacto sobre el valor del contrato entre el cinco (5%) y el quince por ciento (15%).	Incrementa el valor del contrato entre el quince (15%) y el treinta por ciento (30%).	Impacto sobre el valor del contrato en más del treinta por ciento (30%).
	Categoría	Valoración	Insignificante	Menor	Moderado	Mayor	Catastrófico
			1	2	3	4	5
Probabilidad	Raro (puede ocurrir excepcionalmente)	1	2	3	4	5	6
	Improbable (puede ocurrir ocasionalmente)	2	3	4	5	6	7
	Posible (puede ocurrir en cualquier momento futuro)	3	4	5	6	7	8
	Probable (probablemente va a ocurrir)	4	5	6	7	8	9
	Casi cierto (ocurre en la mayoría de circunstancias)	5	6	7	8	9	10

d. Categoría del Riesgo: la valoración completa del Riesgo permite establecer una categoría a cada uno de ellos para su correcta gestión:

Valoración del Riesgo	Categoría
8, 9 y 10	Riesgo extremo
6 y 7	Riesgo alto
5	Riesgo medio
2, 3 y 4	Riesgo bajo

20.6 ASIGNACIÓN Y TRATAMIENTO DE LOS RIESGOS

Debe establecerse un orden de prioridades para:

Evitar el Riesgo
Transferir el Riesgo
Aceptar el Riesgo
Reducir la probabilidad de ocurrencia del evento
Reducir las consecuencias o el impacto del Riesgo a través de planes de contingencia

21. RIESGOS FISCALES

21.1 DEFINICION Y ELEMENTOS DEL RIESGO FISCAL

Teniendo en cuenta la estructura y elementos de la definición de riesgos de la guía, es armónica con la norma ISO 31000, que define riesgo fiscal, así: “Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial”.

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso.

21.2 IDENTIFICACION DE RIESGOS FISCALES

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas:

Los puntos de riesgo**,** son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

Las circunstancias inmediatas, se tratan de aquellas situaciones o actividades bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Identificación de áreas de impacto:

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo. Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Identificación de la causa raíz o potencial hecho generador:

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015). La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio esta tal.

Descripción del riesgo fiscal:

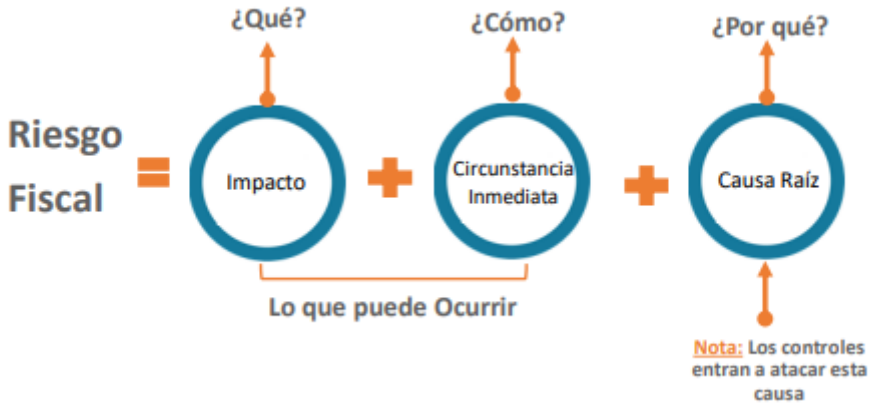
Para redactar un riesgo fiscal se debe tener en cuenta:

✓ Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.

✓ Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

✓ Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.

✓ Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V6 Dirección de Gestión y Desempeño Institucional. Noviembre 2022

21.3 VALORACION DE RIESGOS FISCALES

Evaluación de riesgos:

Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

Probabilidad:

La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según el número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

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

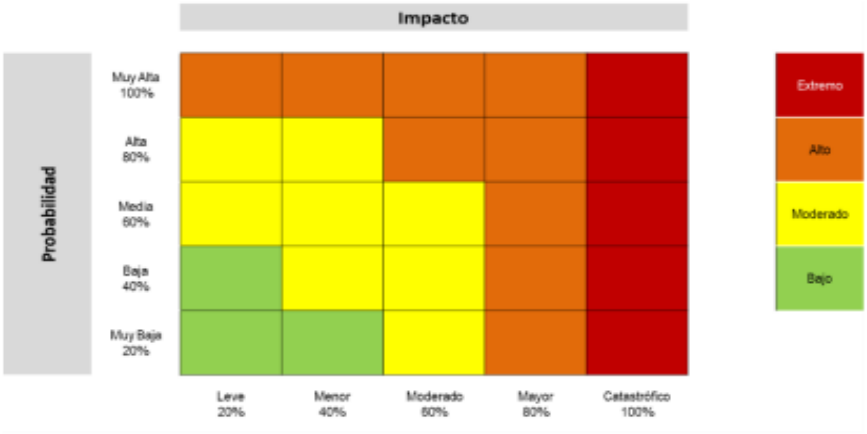
Impacto:

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

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

Determinación del nivel de riesgo inherente

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad.

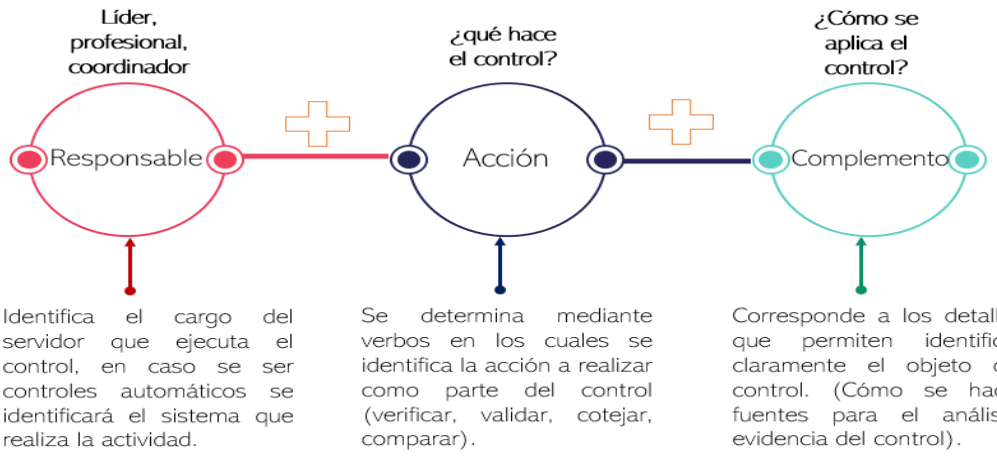


Valoración de controles:

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Se aplican los mismos lineamientos de los riesgos de gestión.

Redacción de Controles:

Una vez determinada la zona de riesgo inherente se definen y valoran los controles aplicables, acorde con las causas definidas, a fin de determinar la zona de riesgo residual. La identificación de controles se debe realizar para cada riesgo a través de las entrevistas con los líderes de los procesos y servidores responsables, será necesario consultar la estructura de operación de la entidad.



Nivel de riesgo (riesgo residual):

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. Se aplican los mismos lineamientos de los riesgos de gestión.

22. REFERENCIAS BIBLIOGRÁFICAS

- Guía para la administración del riesgo y el diseño de controles en entidades públicas V6 Dirección de Gestión y Desempeño Institucional. Noviembre 2022.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas V4 DAFP, Bogotá DC octubre de 2018 y sus anexos.
- Norma ISO 27001:2013. Sistemas de Gestión de la Seguridad de la Información.
- Decreto 1078 de 2015. Estrategia de Gobierno Digital.
- Decreto 1072 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo.
- Documento CONPES 3701 Lineamientos de política para ciberseguridad y ciberdefensa.
- Documento CONPES 3714 de 2011. Del Riesgo Previsible en el Marco de la Política de Contratación Pública.
- GTC 45 de 2012 Guía para la identificación de peligros y valoración de riesgos en seguridad y salud ocupacional.
- Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación. Colombia Compra Eficiente.
- Guía 5. Gestión Clasificación activos (MSPI-Mintic).
- Guía 7. Gestión de riesgos (MSPI - Mintic).
- Guía 8. Controles de seguridad de la información (MSPI - Mintic)
- ANEXO 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas.
- Plan de tratamiento de riesgos de seguridad y privacidad de la información V1.