DIRECCIÓN GENERAL
DE SANIDAD MILITAR
Un equipo humano al servicio de la salud

GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO SSFM DIGSA

2024

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Noviembre 2020	Versión Inicial
2	Octubre 2021	Se aplican los cambios de acuerdo con la normatividad vigente en materia de Gestión del Riesgo.
3	Diciembre 2023	Se adiciona los criterios de identificación, evaluación y definición de controles para los riesgos Fiscales. Se actualiza los criterios para identificación, evaluación y controles riesgos Seguridad de la Información y Corrupción. NOTA PROASIG - PROPLAES: 1. Este documento fue revisado por PROASIG. PROPLAES libera el documento. 2. La información registrada en el documento es responsabilidad del proceso que lo emite. 3. Este documento fue construido de acuerdo con los parámetros de lenguaje claro emitidos por el Departamento Nacional de Planeación.

CONTROL DE APROBACIÓN

Aprobó:	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Alta Dirección	
Revisó:	PD. Julio Cesar Salgado Guerrero Grupo Planeación Estratégica DIGSA Gestor de Calidad	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG
Elaboró:	PD. Julio Cesar Salgado Guerrero Grupo de Planeación Estratégica DIGSA Área Sistemas Integrados de Gestión ARSIG	

- Dirección de Gestión y Desempeño Institucional, diciembre 2020 – DAFP. Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5.

- Dirección de Gestión y Desempeño Institucional noviembre 2022, – DAFP. Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6.

5. GLOSARIO

Acción: Proceso de realización de algo que implica cambio o movimiento. Se determina mediante verbos que indican la acción que deben realizar como parte del control.

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.

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Apetito del Riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionando con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

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

Capacidad del riesgo: Es el máximo valor del novel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Complemento: Detalles que permiten identificar claramente el objeto del control.

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

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

Control: Medida que permite reducir o mitigar el riesgo determinado por el proceso (políticas, dispositivos, prácticas u otras acciones).

Contexto Interno: Determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.

Contexto Externo: Determinan las características o aspectos esenciales del entorno en el cual opera la entidad.

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 la

prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" Capítulo VI. Políticas 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 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- 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.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018.

- Norma Técnica Colombiana NTC ISO 31000 Gestión del Riesgo Principios y Directrices – ICONTEC.

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, si bien es cierto, no desaparecerán totalmente la amenaza o el riesgo, pero sí ayudarán a disminuir o mitigar su probabilidad de ocurrencia y su impacto en el complimiento de los objetivos.

2. OBJETIVO GENERAL

Emitir los lineamientos para la formulación, administración y monitoreo de los riesgos del Subsistema de Salud de las Fuerzas Militares a los que se enfrenta la entidad, que se puedan derivar del aseguramiento y la prestación de los servicios de salud y establecer las actividades necesarias que conduzcan a disminuir la vulnerabilidad frente a situaciones que puedan interferir en el logro de su misionalidad y objetivos estratégicos.

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, contemplada como buenas prácticas en la Gestión del Riesgo; por lo anterior se da continuidad a la política como Subsistema de Salud de las Fuerzas Militares aprobada por los miembros del Subcomité institucional de control interno DIGSA mediante acta No. 0123001426802 MDN-COGFM-JEMCO-DIGSA-GRSYE-22.5 de fecha 19 de Diciembre del 2023.

"El Subsistema de Salud de las Fuerzas Militares, en concordancia con el aseguramiento y prestación de los servicios de Salud, está comprometido en fortalecer su cultura organizacional de la gestión del riesgo, como parte de su mejora continua, a través de la planificación de acciones, seguimiento y la ejecución de controles para reducirlos, compartirlos y asumirlos. Para tal efecto, realiza la identificación, análisis, valoración e intervención de éstos en alineación con el Sistema Integrado de Gestión".

4. FUNDAMENTO NORMATIVO

- 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.

- 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

Contenido

entidad.

Contexto del Proceso: Determinan las características o aspectos esenciales del proceso y sus interrelaciones.

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

Factores de riesgo: Son las fuentes generadoras de riesgos.

Integridad: Propiedad de exactitud y completitud.

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

Mapa de riesgos: Documento que consolida la información resultante en cada una de las etapas de la Gestión del riesgo.

Nivel del Riesgo: Es el valor que se determina a partir de combinar la ocurrencia de la probabilidad y el impacto sobre la capacidad de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo de obtiene de multiplica la 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 dentro de la matriz de calor.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad y estará asociada a la exposición al riesgo del proceso o actividad que se está analizando.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

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

Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo inherente: Nivel del riesgo propio de la actividad, es aquel al que se enfrenta la entidad en ausencia de acciones para modificar su probabilidad o impacto.

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.

Riesgo residual: Es el resultado de aplicar la efectividad de los controles o medidas de tratamiento al riesgo inherente.

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.

Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales

(probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

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".

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 (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique).

Recurso público: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.

Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07).

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).

Tolerancia al riesgo: Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Vulnerabilidad: Es una debilidad, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

6. ADMINISTRACIÓN DEL RIESGO

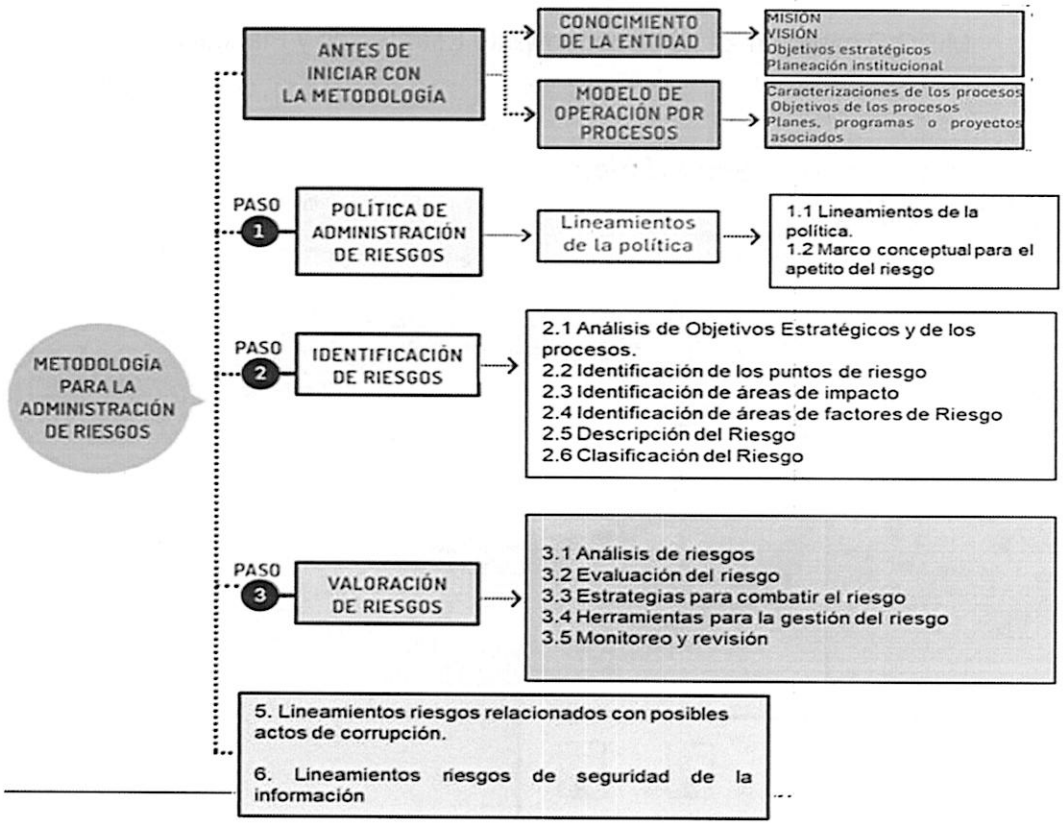
Es una tarea propia de la alta dirección de la entidad y se desarrolla desde el ejercicio de Direccionamiento Estratégico y de Planeación Dimensión 2 de MIPG, en alineación a la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP. En este sentido, la identificación y valoración de los riegos se integra en el desarrollo de la estrategia, la formulación de los objetivos e implementación de esto a través de la toma de decisiones; por lo tanto, mediante la Guía para la Administración del Riego del SSFM se definen los lineamientos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos de la entidad.

MIPG Dimensión 2 - Direccionamiento Estratégico y Planeación

Fuente: Manual Operativo MIPG – DAFP

7. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

De acuerdo con el Departamento Administrativo de la Función Pública, para la adecuada aplicación de la metodología de la administración del riesgo, es indispensable conocer la entidad y el modelo de operación por procesos como se indica en el siguiente esquema que presenta la metodología para la administración del riesgo



Fuente: Departamento Administrativo de la Función Pública, Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 5. Bogotá, Colombia. 2020.

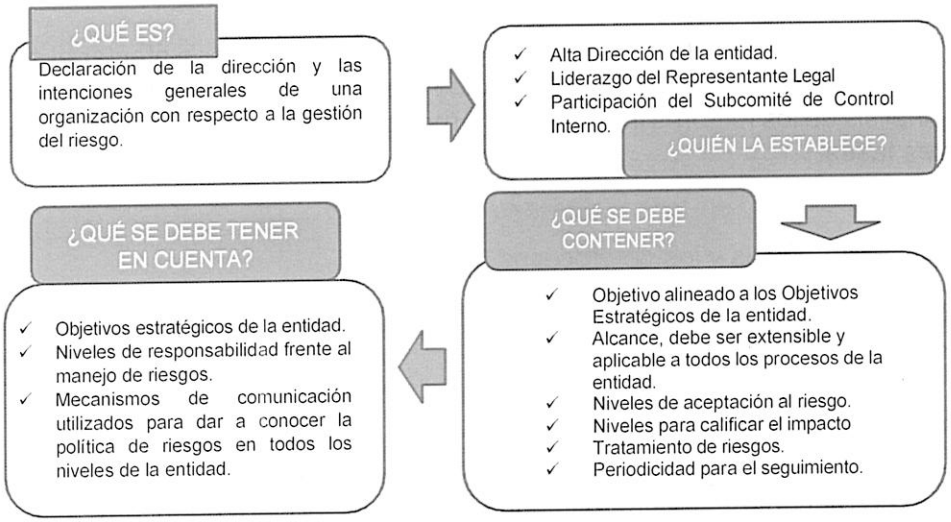
Para la formulación y puesta en marcha de la metodología para la administración del riesgo es fundamental tener un amplio conocimiento de la entidad, en cuanto a misión, visión, objetivos estratégicos, estructura y cultura organizacional, interrelación de procesos, entre otros aspectos. Seguidamente, para la definición de lineamientos en materia del riesgo se aplicarán los 3 paso definidos en la metodología.

8. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

El Subsistema de Salud de las Fuerzas Militares, en concordancia con el aseguramiento y prestación de los servicios de Salud, está comprometido en la administración de los riesgos institucionales de Gestión, Corrupción, Fiscales y de Seguridad de la Información alineados a los Planes institucionales, estratégicos y proyectos, de acuerdo a la guía para la administración del riesgos del Subsistema de Salud de las Fuerzas Militares DIGSA, estableciendo acciones de control preventivas, detectivas y correctivas que permitan la mitigación y acción frente a la posibilidad de materialización de sus riesgos, garantizando la continuidad de sus servicios y el logro de los objetivos.

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

Elementos Política de Administración del riesgo



Fuente: Adoptado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas 6.0 por el Grupo de Planeación – Desarrollo Institucional de la DIGSA.

La sumatoria de estos elementos son la base para la elaboración de los lineamientos de la política de administración del riesgo, la cual debe considerar el apetito del riesgo como insumo del análisis de la entidad, partiendo de los siguientes componentes:

Marco conceptual para el apetito del riesgo

9. IDENTIFICACIÓN DEL RIESGO

Es la etapa inicial, con la cual se busca identificar los riesgos que pueden llegar a afectar el cumplimiento de los objetivos, para ello se debe tener en cuenta el contexto estratégico de la entidad, la caracterización de cada proceso, y el análisis de los factores internos y externos que impacten en el logro de los objetivos, aplicando las siguientes fases:

Análisis de los Objetivos Estratégicos y los de procesos

Consiente en identificar el impacto que tiene el riesgo frente al objetivos estratégicos de la entidad o del proceso.

Identificación de los puntos de riesgo

Son las actividades que se realizan y su interacción, donde existe evidencia o se tiene indicios de que puede ocurrir eventos de riesgo operativo, evaluando su probabilidad de ocurrencia, severidad, estructuración de acciones preventivas y mitigación para asegurar el cumplimiento de los objetivos.

Identificación de áreas de impacto

Es la exposición a la que la entidad se somete si llegara a materializarse el riesgo, generando afectaciones económicas o reputacionales.

Identificación de áreas de factores de riesgo:

Son los factores generadores de riesgos que afectan la complejidad al interior y exterior de la entidad:

- Procesos.
- Talento Humano.
- Económico y Financiero.
- Estratégicos.
- Tecnológicos.
- Infraestructura.
- Políticos.
- Ambientales.
- Legales y reglamentarios.
- Comunicación Interna.
- Situaciones externas que afectan a la entidad.

Identificación Riesgos de Gestión

El Coordinador y líder de proceso, apoyado con su equipo de trabajo realizara el análisis del contexto interno y externo con el fin de determinar las posibles acciones que puedan afectar el cumplimiento de sus objetivos, este análisis es la base para la identificación de los riesgos, todo lo anterior asociado a los factores de riesgo los cuales tendrán una relación con la clasificación de riesgo, la estructura que propone la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Versión 6, se describe a continuación.

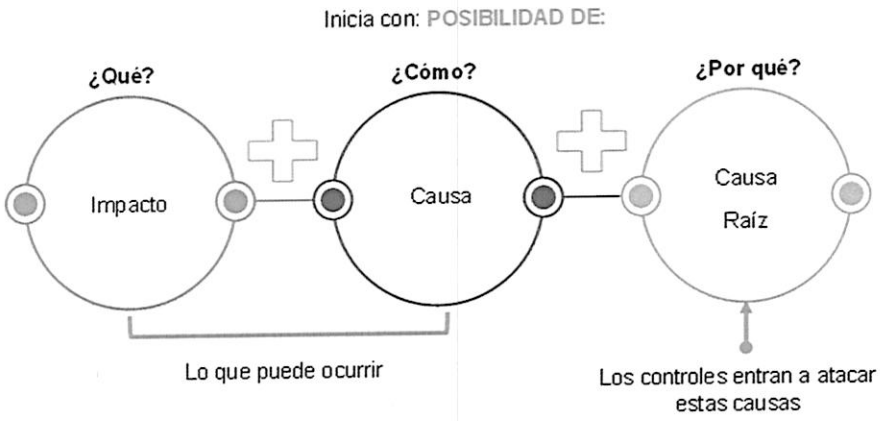
La descripción del riesgo debe ser detallada y clara, de modo que su comprensión sea entendible para todos los involucrados y puedan participar planteando acciones de tratamiento. Las preguntas claves que se deben determinar al momento de la redacción del riesgo:

a) ¿QUÉ?: Identificar el impacto o afectación en el cumplimiento del objetivo.

b) ¿CÓMO?: Establecer las causas inmediatas a partir de los factores determinados en el contexto.

c) ¿POR QUÈ?: Establece la causa raíz, por la cual se presenta el riesgo, en este paso pueden existir una o más causas, que son la base para la definición de los controles para la mitigación y tratamiento del riesgo.

Estructura propuesta para la redacción de riesgos de Gestión



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

Al momento de redactar el riesgo es importante aplicar premisas como son:
Evitar la negación para expresar el riesgo mediante palabras que denoten factor de riesgo, como, por ejemplo:

- "No…", "Que no…" "ausencia de", "falta de", "poco(a)", "escaso(a)", "insuficiente", "deficiente", "debilidades en…"[1] .
- Sanciones al presupuesto por falla en la asignación del recurso durante la vigencia.

No se debe confundir la causa como riesgo.

- Ejemplo: Ausencia de lineamientos para la formulación, implementación y seguimiento a los planes.

La descripción del riesgo no debe ser la debilidad de un control.

- Ejemplo: La no inactivación de los accesos y permisos de los usuarios de la DIGSA a la plataforma tecnológica por no contar con el reporte de novedades de Talento Humano.

Los riesgos transversales NO existen, lo que existe son causas transversales que afectan el desarrollo de las actividades de la entidad, los cuales están asociadas a la Gestión Documental, Gestión Contractual y Gestión jurídica, sin embargo, los controles para la mitigación son diferentes.

Identificación del riesgo de seguridad de la información

En la identificación de los riesgos de seguridad de la información se debe tener en cuenta que deben tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información, el cual debe estar alineado con el marco de referencia de arquitectura TI, soportando transversalmente los demás habilitadores de la Política de gobierno digital (Seguridad de la Información, Arquitectura, Servicio Ciudadano Digitales), su identificación será liderada por el Grupo Sistema Integral de Información – Tecnologías de la Información y Comunicaciones SISAM, quien en conjunto con los Coordinadores y lideres, equipo de trabajo realizaran la construcción del mapa de riesgos se Seguridad de la Información, y posterior consolidación por parte del Grupo de Planeación Estratégica GRUPL.

El primer paro que se debe realizar es la identificación de los activos de información dentro de los procesos, definimos como un activo de información cualquier elemento que participe en el tratamiento de información que tenga valor para la entidad. Sin embargo, en el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la entidad pública, servicios Web, redes, información digital, personal, ubicación, organización, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO- que utiliza la entidad para su funcionamiento, lo anterior acorde a los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 4 del 2018, para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas".

---

[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. 27p

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información: **Pérdida de la confidencialidad, Pérdida de la integridad, Pérdida de la disponibilidad**, estos a su vez tienen que estar asociados al grupo de activos o activos específicos identificados por cada proceso y a la vez analizar las posibles amenazas y vulnerabilidad que podrían causar su materialización, lo anterior acorde a los anexos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 4 del 2018.

Identificación del riesgo de Corrupción

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, su revisión o actualización debe ser anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo o en aquellos casos que se requiera es necesario que en la descripción del riesgo concurran los componentes de su definición, así: **Acción u omisión + Uso del poder + Desviar la gestión de lo público + Beneficio privado**, para su construcción se tendrán en cuenta los lineamientos establecidos s en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018.

Identificación del riesgo Fiscal

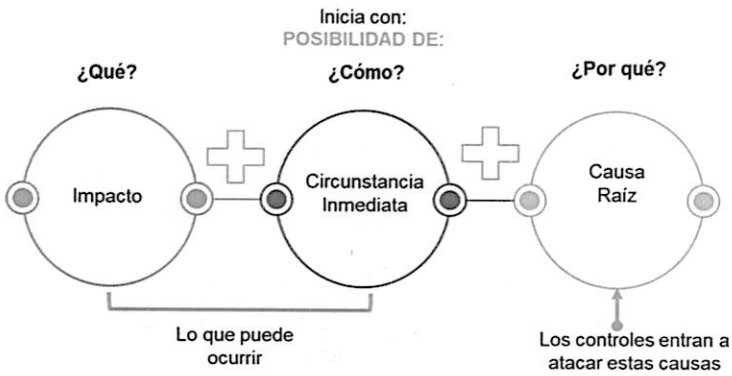
El primer paso para la identificación de los riesgos fiscales es establecer los puntos de riesgos fiscales y que circunstancias inmediatas se generaría por una posible materialización, estos puntos de riesgos son las diferentes situaciones que se generan en el desarrollo de las actividades de la administración, gestión, ejecución, adquisición, manejo, planeación, custodia, conservación, enajenación, consumo, adjudicación, gastos, inversión, y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas, lo anterior acorde a los lineamientos establecidos en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, con lo anterior la estructura y elementos en la definición de los riesgos se enmarca en la marca en los siguiente definición, ***Efecto dañoso sobre recursos públicos o bienes o interés patrimoniales de naturaleza pública, a causa de un evento potencial***, como efecto se define el daño que se pueda generar sobre los recursos públicos y/o bienes y/o intereses patrimoniales de naturaleza publica y evento potencial son los hechos inciertos o incertidumbres, en lo que se relaciona con acción u omisión hace referencia al daño que podría generar sobre los recursos públicos y/o bienes y/o intereses patrimoniales de naturaleza pública.

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.

Estructura propuesta para la redacción de riesgos fiscales



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

10. VALORACIÓN DEL RIESGO

En esta etapa, se determina 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, con el fin de determinar la zona de riesgo inicial (Riesgo Inherente).

Probabilidad e Impacto Riesgos de Gestión – Riesgos Seguridad de la Información - Riesgos Fiscales

Con el fin establecer la ocurrencia del riesgo, con relación a las causas y consecuencias que potencialmente tendría del riesgo en su etapa inicial - Riesgo Inherente, se debe:

Evaluar la exposición del riesgo, asociada al proceso o actividad que se esté analizado, es decir, número de veces que se pasa por el punto de riesgo en el periodo de 1 año según su clasificación, los criterios para calificar el nivel de la probabilidad se definen en la siguiente tabla, así:

Criterios para Calificar la Probabilidad

Criterio	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%

Criterio	Frecuencia de la actividad	Probabilidad
Muy Alta	La actividad que conlleva el riesgo se ejecuta más 5000 veces por año.	100%

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

Calcular el Impacto según el grado en que las consecuencias o efectos pueden perjudicar a la entidad al materializarse el riesgo. Con el fin de brindar herramientas que les permitan a los procesos ubicarse con mayor claridad en la escala de impacto, se utilizaran las variables en términos económicos y reputacionales, para los riesgos fiscales es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública.

Criterios para Calificar el Impacto

Criterio	Afectación Económica	Reputacional
Insignificante 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 e 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.
Catastrófico0%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

Probabilidad e Impacto Riesgos de Corrupción

Análisis de la probabilidad

La probabilidad de ocurrencia del riesgo se expresa en términos de frecuencia o factibilidad, la frecuencia analiza el numero de eventos que se puedan presentar en un periodo determinado, esto asociados a la materialización o alguna situación o evento asociado a actos de corrupción. La factibilidad se expresa en los factores externos e internos que puedan llevar a un posible hecho de corrupción que pueda suceder.

Criterio	Descripción	Frecuencia
Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas de 1 vez al año
Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.

Criterio	Descripción	Frecuencia
Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años
Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
Muy Alta	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

Aunque se utilice el mismo mapa de calor para los riesgos de gestión, para los riesgos de corrupción la calificación del impacto se calcula mediante la siguiente tabla.

Criterios para calificar el Impacto - Riesgo de Corrupción

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			

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

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

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

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

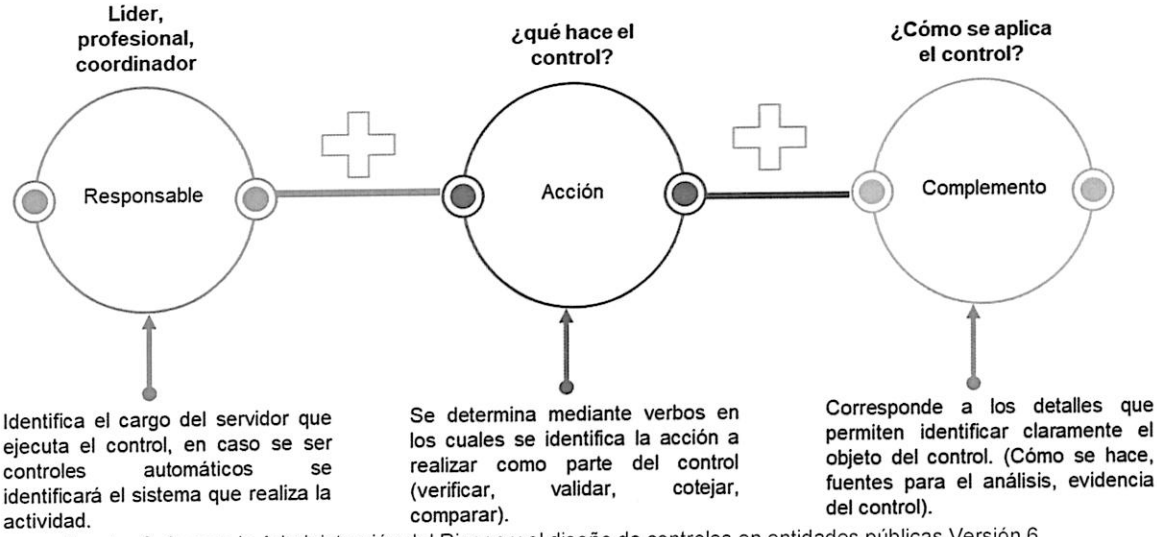
Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos.

11. IDENTIFICACIÓN DE CONTROLES Y VALORACIÓN DEL RIESGOS RESIDUAL

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

Los elementos para la descripción de los controles están directamente relacionados con el responsable de ejecutar el control, la acción y el complemento, que permitirán entender su tipología y particularidades para su valoración. Una vez determinada la zona de riesgo inherentes 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. Con lo anterior la estructura que se determina para la elaboración del control debe cumplir con los siguientes criterios.

Estructura propuesta para la Redacción del Control



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

Tipología de los controles:

Los controles se clasifican de acuerdo con su naturaleza, en:

- Preventivo: Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización, y está asociado con la entrada del proceso antes de realizar la actividad.

- Detectivo: Aquellos que detectan que algo ocurre y devuelven el proceso a los controles preventivos, atacan la probabilidad de ocurrencia. Se activa durante la ejecución del proceso, puede generar reprocesos.

- Correctivo: 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, control accionado en la salida del proceso.

Así mismo y de acuerdo con la forma como se ejecuta el control puede ser:

- Manual: ejecutado por personas.
- Automático: ejecutado sistemáticamente.

Características del control:

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

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.

Controles Riesgos Seguridad de la Información

Para la identificación de controles a nivel de riesgos de seguridad de la Información se deberá implementar de acuerdo con el Anexo 1 Modelo de Seguridad y Privacidad de la Información, el cual dentro de su contenido establece los controles y objetivos que se deben implementar acorde al anexo A de la norma NTC: ISO/IEC 27001.

12. 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, Seguridad Digital y Fiscales, así como la relación costo-beneficio de las medidas de tratamiento.

Por lo anterior se deberá seleccionar una sola de las siguientes opciones de tratamiento definidas en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6.

- Aceptar: Si el nivel de riesgo se encuentra en una zona inherente Baja y cumple con los criterios de aceptación, no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. *(Ningún riesgo de corrupción podrá ser aceptado).*

- Evitar: Cuando los escenarios de riesgo identificados se consideran demasiado extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.

- Compartir el riesgo: Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionar, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

- Reducir el riesgo: El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

13. 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, Seguridad Digital y Fiscales, 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.

Acciones para 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 los entes de control 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.
- Llevar a cabo un monitoreo permanente.

14. 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 se describe a continuación.

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 Gestión, Corrupción Seguridad de la Información, y Fiscales 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.

Línea Estratégica

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	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

LÍNEA ESTRATÉGICA	
acuerdo con la política de administración del riesgo establecida y aprobada.	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.	

Primera Línea de Defensa

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,	

PRIMERA LÍNEA DE DEFENSA	
Segunda y Tercer Línea de Defensa con relación a la Gestión de Riesgos.	

Segunda Línea de Defensa

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.
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.

Tercera Línea de Defensa

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	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.

TERCERA LÍNEA DE DEFENSA	
identifiquen y actualicen las matrices de riesgos por parte de los responsables.	
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.

15. 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 con lo establecido en los controles, lo anterior realizado en el Sistema Información Suite Visión establecido por la Dirección General de Sanidad Militar DIGSA.

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	Mensual
Seguridad Digital	Trimestral
Fiscal	Trimestral

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 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:

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, teniendo en cuenta el seguimiento del Plan Anticorrupción y Atención al Ciudadano se realizara cuatrimestralmente de acuerdo con los siguientes criterios.

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

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

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