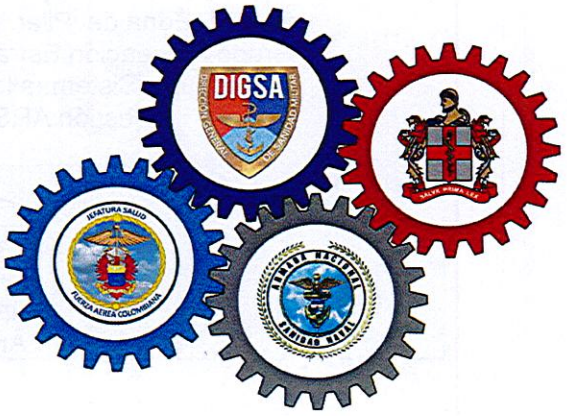
Guía para la Administración del Riesgo SSFM DIGSA

Un equipo humano al servicio de la salud



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. NOTA PROASIG - PROPLAES: 1. Este documento fue revisado por PROASIG, cumple con los requisitos establecidos en el formato establecido por el Sistema Integrado de Gestión SIG, para aprobarlo en la SVE; PROPLAES libera el documento. 2. Dada la reestructuración de la DIGSA, se ajustaron las políticas de operación para el control de la información documentada de los procesos para el SIG. 3.La información registrada en el documento es responsabilidad del proceso que lo emite.

CONTROL DE APROBACIÓN

Aprobó:	PD. Alexandra Martinez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección	
Revisó:	TASD. Nidia Liliana Guerrero Santos Grupo Planeación Estratégica DIGSA Gestor de Calidad Área Desarrollo Institucional ARDEI	
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG	PD. Mónica Bibiana Bustamante Rondon Grupo Planeación Estratégica DIGSA Área Desarrollo Institucional ARDEI
Elaboró:	TASD. Nidia Liliana Guerrero Santos Grupo de Planeación Estratègica DIGSA Área Desarrollo Institucional ARDEI	

TABLA DE CONTENIDO

I. PRESENTACIÓN 4
II. OBJETIVO GENERAL 4
III. ALCANCE 4
IV. FUNDAMENTO NORMATIVO 4
V. CONCEPTOS BASICOS 6
VI. ADMINISTRACIÓN DEL RIESGO 7
VII. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO 8
1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 9
2. IDENTIFICACIÓN DEL RIESGO 10
2.1 Análisis de los Objetivos Estratégicos y los de procesos: 11
2.2 Identificación de los puntos de riesgo: 11
2.3 Identificación de áreas de impacto: 11
2.4 Identificación de áreas de factores de riesgo: 11
2.4.1 Identificación del riesgo de seguridad de la información: 11
2.5 Descripción del Riesgo: 12
2.5.1 Descripción de los riesgos de Corrupción 13
2.6 Clasificación del Riesgo 13
3. VALORACIÓN DEL RIESGO 15
3.1. Análisis del riesgo 15
3.2. Evaluación del riesgo 17
a. Matriz de Calor o Mapa de Calificación 17
b. Valoración de Controles 19
c. Estructura para de la definición del control: 19
d. Tipología de los controles: 19
e. Análisis y evaluación de los controles: 20
f. Nivel del riesgo (riesgo Residual) 21
g. Plan de Contingencia: 22
3.3. Manejo o Tratamiento del Riesgo: 23
3.4. Herramientas para la gestión del riesgo: 23
3.5. Monitoreo y Seguimiento 24
a. Modelo de las líneas de defensa 24
b. Responsable de Seguridad de la información 25
c. Monitoreo 25
d. Seguimiento 25
ANEXOS 27
BIBLIOGRAFÍA 28

TABLA DE FIGURAS

Figura 1. MIPG Dimensión 2 - Direccionamiento Estratégico y Planeación 8
Figura 2. Metodología para la Administración del Riesgo 9
Figura 3. Elementos Política de Administración del riesgo. 9
Figura 4. Marco conceptual para el apetito del riesgo 10
Figura 5. Fases de la Identificación del Riesgo. 10
Figura 6. Componentes de la definición del riesgo de corrupción 13
Figura 7. Estructura Zona riesgo inicial – Riesgo Inherente 15
Figura 8. Matriz de calor 18
Figura 9. Matriz de calor – Riesgo Inherente 18
Figura 10. Estructura Zona riesgo inicial – Riesgo Inherente 19
Figura 11. Matriz de calor – Riesgo Residual 22
Figura 12. Estrategias para el manejo del riesgo 23

INDICE DE TABLAS

Tabla 1. Factores de Riesgo y Clasificación del Riesgo 14
Tabla 2. Criterios para Calificar la Probabilidad 15
Tabla 3. Criterios para Calificar el Impacto 16
Tabla 4. Criterios para calificar el Impacto - Riesgo de Corrupción 16
Tabla 5. Atributos del diseño del control 20
Tabla 6. Control vs. Atributos 21
Tabla 7. Líneas de Defensa, Rol y Responsabilidad 24
Tabla 8. Tiempos para el desarrollo del Monitoreo 25

I. 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.

II. 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.

III. ALCANCE

Orientar a todos los actores del Subsistema de Salud de las Fuerzas Militares, para la administración del riesgo, teniendo como fundamentos la metodología definida por el Departamento Administrativo de la Función Pública -DAFP y la Norma Técnica Internacional ISO 31000:2018, contemplada como buenas prácticas en la Gestión del Riesgo; 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. 0120009584902 de fecha 19 de noviembre del 2020.

"*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*".

IV. FUNDAMENTO NORMATIVO

FECHA	DESCRIPCIÓN
Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. Art. 2. Objetivos del Sistema de Control Interno. a) Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan, Literal f) Definir y aplicar medidas para prevenir los riesgos, detectar

FECHA	DESCRIPCIÓN
	y corregir las desviaciones que se presenten en la organización y que pueden afectar el logro de los objetivos. 4 literal a): toda entidad debe establecer objetivos y metas tanto generales como específicas, así como la formulación de los Planes Operativos que sean necesarios.
Ley 352 de 1997	Por la cual se reestructura el Sistema de Salud y se dictan otras disposiciones en materia de Seguridad Social para las Fuerzas Militares y la Policía Nacional.
Ley 1474 de 2011	"Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" Capítulo VI. Políticas institucionales y pedagógicas. Artículo 73. Plan Anticorrupción y de Atención al Ciudadano. Artículo 74. Plan de Acción de las entidades Públicas.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1955 de 2019	Por la cual se expide el Plan Nacional de Desarrollo 2018 – 2022, Pacto por Colombia Pacto por la Equidad, marco normativo que servirá a este Gobierno para impulsar su propuesta de desarrollo
Decreto 2641 de 2012	"Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011". Artículo 7: Las entidades del orden nacional, departamental y municipal deberán publicar en un medio de fácil acceso al ciudadano su Plan Anticorrupción y de Atención al Ciudadano a más tardar el 31 de enero de cada año.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", Capítulo 3 Sistema Institucional y Nacional de Control Interno." Artículo 2.2.21.5.4 Administración de riesgos. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo.
Decreto 338 de 2019	"Por el cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción". Capítulo 7 Red Anticorrupción. Artículo 2.2.21.7.1. Creación de la Red Anticorrupción. Crease la Red Anticorrupción integrada por los jefes de Control Interno o quien haga sus veces para articular acciones oportunas y eficaces en la identificación de casos o riesgos de corrupción en instituciones públicas, para generar las alertas de carácter preventivo frente a las decisiones de la administración, promoviendo la transparencia y la rendición de cuentas en la gestión pública.

FECHA	DESCRIPCIÓN
Acuerdo No 36 de 2003 del CSSMP	"Por el cual se establecen políticas generales para orientar una efectiva gestión del SSMP"
Acuerdo No 37 de 2003 del CSSMP	"Por el cual se establecen normas para el control y evaluación de la gestión en el SSMP".
Norma Técnica Colombiana NTC ISO 31000	Gestión del Riesgo Principios y Directrices – ICONTEC.
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.

V. CONCEPTOS BASICOS

CONCEPTO	DESCRIPCIÓN
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.

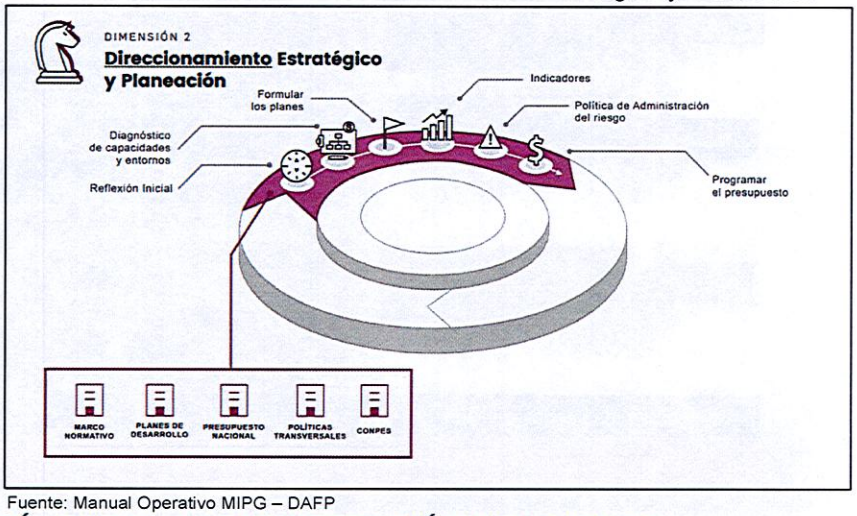
CONCEPTO	DESCRIPCIÓN
Contexto estratégico:	Son las condiciones externas e internas del entorno que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de la entidad.
Contexto del Proceso:	Determinan las características o aspectos esenciales 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,
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

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

VI.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.

Figura 1. MIPG Dimensión 2 - Direccionamiento Estratégico y Planeación



Fuente: Manual Operativo MIPG – DAFP

VII. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

De acuerdo con el Departamento Administrativo de la Función Pública[1], para la adecuada aplicación de la metodología de la administración del riesgo, es indispensable conocer la entidad y el modelo de operación por procesos como se indica en el siguiente esquema que presenta la metodología para la administración del riesgo figura 2.

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.

[1] 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. 20p.

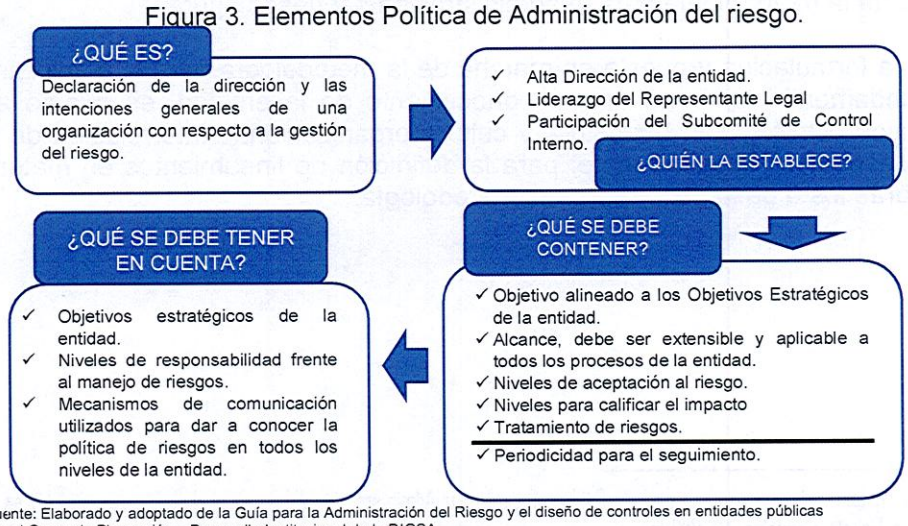
Figura 2. Metodología para la Administración del Riesgo

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

1. *POLÍTICA DE ADMINISTRACIÓN DEL RIESGO*

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

Figura 3. Elementos Política de Administración del riesgo.



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

[2] 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. 21p

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

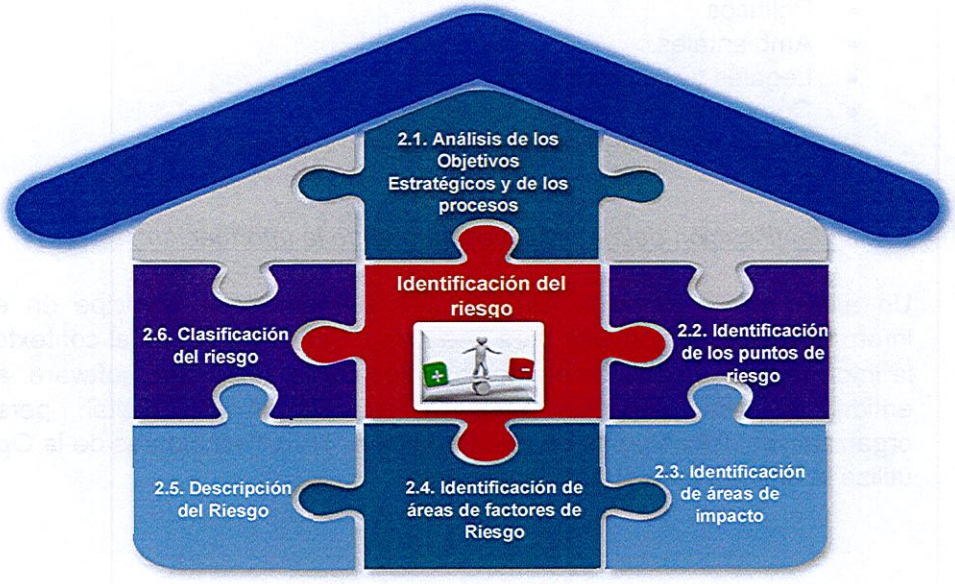
Figura 4. Marco conceptual para el apetito del riesgo

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

2. 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:

Figura 5. Fases de la Identificación del Riesgo.



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

2.1 *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.

2.2 *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.

2.3 *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.

2.4 *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.

2.4.1 *Identificación del riesgo de seguridad de la información*[3]*:*

Un activo de información es 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.

[3] Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (Anexo 4 – DAFP) versión 2. Bogotá. Colombia 2019. 12p.

Es necesario que la entidad identifique los activos de información y documente un inventario de activos, para así poder determinar lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (Front Office), en alineación con el Plan del tratamiento de riesgos de seguridad y privacidad de la información definido por la entidad.

2.5 *Descripción del Riesgo*:

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.

Ejemplo:

Redacción	¿Qué? = Impacto	¿Cómo? = Causa Inmediata	¿Por qué? = Causa Raíz
Posibilidad de:	Afectación jurídica	Uso de normativa desactualizada o derogada	Elaboración de conceptos jurídicos erróneamente fundamentados.

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

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…"[4] .
  - Sanciones al presupuesto por falla en la asignación del recurso durante la vigencia.
- No se debe confundir la causa como riesgo.

[4] 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

- 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.

2.5.1 *Descripción de los riesgos 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, y contemplar los cuatro (4) componentes de la figura 6. 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[5].

Figura 6. Componentes de la definición del riesgo de corrupción

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

2.6 *Clasificación del Riesgo*

Los riesgos se deben agrupar de acuerdo con la clasificación que establece el Departamento Administrativo de la Función Pública[6] y su interacción frente a los factores de riesgo definidos por la entidad:

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

[6] 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. 35p.

Tabla 1. Factores de Riesgo y Clasificación del Riesgo

Clasificaciòn	Descripciòn	Factores (Internos – Externos)
Ejecución y administración de procesos:	Pérdidas derivadas de errores en la ejecución y administración de procesos.	Procesos: •Falta de procedimientos. •Errores de grabación, autorización. •Errores en calculos para pagos internos y externos. •Falta de capacitación, temas relacionados con el personal.
Fraude externo:	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	Evento Externo: •Suplantación de identidades. •Asalto a la oficina. •Atentados, vandalismo, orden público.
Fraude interno:	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.	Talento Humano. •Hurto activos. •Posibles comportamientos no éticos de los empleados. •Fraude interno (corrupción, soborno). •Incluye seguridad y salud en el trabajo.
Fallas tecnológicas:	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.	Tecnológia: •Daño de equipos. •Caída de aplicaciones. •Caída de redes. •Errores en programas.
Relaciones laborales:	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.	•Comunicación Interna. •Legales y reglamentarios. •Talento Humano.
Usuarios, productos y prácticas:	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.	•Comunicación Interna. •Legales y reglamentarios. •Talento Humano.
Daños a activos fijos/ eventos externos:	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.	Infraestructura •Derrumbes •Incendios •Inundaciones •Daños a activos fijos.
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.	•Infraestructura •Evententos externos •Tecnologicos

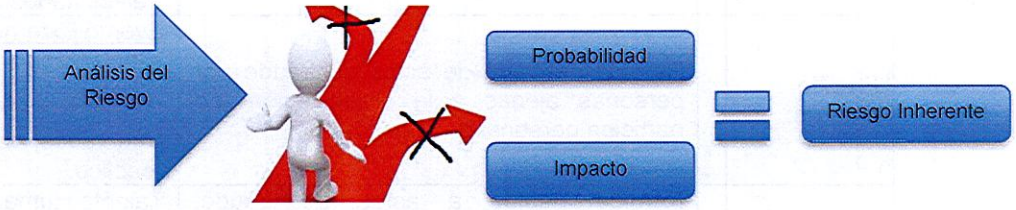
Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – 35 y 36 p.

3. 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)

3.1. Análisis del riesgo

Figura 7. Estructura Zona riesgo inicial – Riesgo Inherente



Fuente: Elaborado por el Grupo de Planeación – Desarrollo Institucional de la DIGSA.

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:

1. 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[7] según su clasificación, los criterios para calificar el nivel de la probabilidad se definen en la tabla 2, así:

Tabla 2. 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%
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 – 39 p.

2. 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.

[7] 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. 38p.

Tabla 3. 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 – 40 p.

Aunque se utilice el mismo mapa de calor, para los riesgos de corrupción la calificación del impacto se calcula mediante la tabla 4. La probabilidad de los riesgos de corrupción se califica con los mismos cinco niveles de los demás riesgos.

Tabla 4. 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			

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

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.

El procesamiento de los datos descritos en los puntos 2 y 3 propios del riesgo inherente, permite conocer la ubicación del riesgo dentro de la matriz de calor, como se muestra en el ejemplo a continuación:

Riesgo: Posibilidad de afectación jurídica, por uso de normativa desactualizada o derogada en la elaboración de conceptos jurídicos erróneamente fundamentados.

Criterio Probabilidad:

Número de veces que desarrolla la actividad: 30 veces en el mes = 360 respuestas de gestión legal (30 *12= 360).

Criterio de Impacto:

Cálculo económico: Si se llegara a materializar tendría una afectación entre 100 y 500 SMLMV.

Calculo Reputacional: Si el riesgo se materializara, la entidad tendría una afectación de la imagen con efecto publicitario.

Dando como resultado Riesgo Inherente:

Probabilidad inherente = media 60%

Impacto inherente = mayor 80%

3.2. Evaluación del riesgo

El objetivo de la evaluación del riesgo es facilitar la toma de decisiones, basado en los resultados del análisis acerca de cuáles riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento, teniendo como apoyo la matriz de calor.

a. Matriz de Calor o Mapa de Calificación

La Matriz de calor está conformada por dos ejes (X y Y), donde el eje X representa la probabilidad de frecuencia y el eje Y representa el impacto, definiendo mediante el punto de intersección la zona de severidad del Riesgo Inherente.

Figura 8. Matriz de calor

PROBABILIDAD	ZONA DE RIESGO				
MUY ALTA 100	ZONA DE RIESGO ALTA 2000	ZONA DE RIESGO ALTA 4000 4000	ZONA DE RIESGO ALTA 6000 6000	ZONA DE RIESGO ALTA 8000	ZONA DE RIESGO EXTREMA 10000
ALTA 80	ZONA DE RIESGO MODERADA 1600	ZONA DE RIESGO MODERADA 3200	ZONA DE RIESGO ALTA 4800	ZONA DE RIESGO ALTA 6400	ZONA DE RIESGO EXTREMA 8000
MEDIA 60	ZONA DE RIESGO MODERADA 1200	ZONA DE RIESGO MODERADA 2400	ZONA DE RIESGO MODERADA 3600	ZONA DE RIESGO ALTA 4800	ZONA DE RIESGO EXTREMA 6000
BAJA 40	ZONA DE RIESGO BAJA 800	ZONA DE RIESGO MODERADA 1600	ZONA DE RIESGO MODERADA 2400	ZONA DE RIESGO ALTA 3200	ZONA DE RIESGO EXTREMA 4000
MUY BAJA 20	ZONA DE RIESGO BAJA 400	ZONA DE RIESGO BAJA 800	ZONA DE RIESGO MODERADA 1200	ZONA DE RIESGO ALTA 1600	ZONA DE RIESGO EXTREMA 2000
IMPACTO	20 INSIGNIFICANTE	40 MENOR	60 MODERADO	80 MAYOR	100 CATASTRÓFICO

Fuente: Elaborado por el Grupo de Planeación – Desarrollo Institucional de la DIGSA.

Extendiendo el ejemplo, el cruce de los datos de la probabilidad e impacto define dentro de la Matriz de Calor la zona de riesgo Alta, así:

Riesgo: Posibilidad de afectación jurídica, por uso de normativa desactualizada o derogada en la elaboración de conceptos jurídicos erróneamente fundamentados.

Dando como resultado Riesgo Inherente:

Probabilidad inherente = media 60% * Impacto inherente = mayor 80% = Zona de Riesgo Alta.

Figura 9. Matriz de calor – Riesgo Inherente

PROBABILIDAD	ZONA DE RIESGO				
MUY ALTA 100	ZONA DE RIESGO ALTA 2000	ZONA DE RIESGO ALTA 4000 4000	ZONA DE RIESGO ALTA 6000 6000	ZONA DE RIESGO ALTA 8000	ZONA DE RIESGO EXTREMA 10000
ALTA 80	ZONA DE RIESGO MODERADA 1600	ZONA DE RIESGO MODERADA 3200	ZONA DE RIESGO ALTA 4800	ZONA DE RIESGO ALTA 6400	ZONA DE RIESGO EXTREMA 8000
MEDIA 60	ZONA DE RIESGO 1200	ZONA DE RIESGO MODERADA 2400	ZONA DE RIESGO MODERADA 3600	ZONA DE RIESGO ALTA 4800	ZONA DE RIESGO EXTREMA 6000
BAJA 40	ZONA DE RIESGO BAJA 800	ZONA DE RIESGO MODERADA 1600	ZONA DE RIESGO MODERADA 2400	ESGO ALTA 3200	ZONA DE RIESGO EXTREMA 4000
MUY BAJA 20	ZONA DE RIESGO BAJA 400	ZONA DE RIESGO BAJA 800	ZONA DE RIESGO MODERADA 1200	ESGO ALTA 1600	ZONA DE RIESGO EXTREMA 2000
IMPACTO	20 INSIGNIFICANTE	40 MENOR	60 MODERADO	80 MAYOR	100 CATASTRÓFICO

Fuente: Elaborado por el Grupo de Planeación – Desarrollo Institucional de la DIGSA.

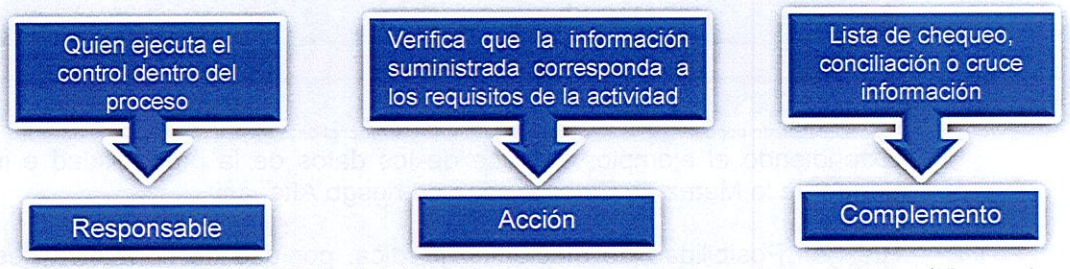
b. Valoración de Controles

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).

c. Estructura para de la definición del control:

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.

Figura 10. Estructura Zona riesgo inicial – Riesgo Inherente



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

d. Tipología de los controles:

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

- ✓ Preventivos: 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.

- ✓ Detectivos: 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.

- ✓ Correctivos: Aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia, 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.

e. Análisis y evaluación de los controles:

Los controles se diseñan mediante los atributos (Eficiencia o informativos), teniendo en cuenta características relacionadas con la eficiencia y la formalización[8], como se muestra a continuación:

Tabla 5. Atributos del diseño del control

CARACTERÍSTICAS			DESCRIPCIÓN	PESO
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permite reducir el impacto de la materialización del riesgo, tiene 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.	

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 5. 46p.

[8] 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. 45p

A partir del comportamiento de los controles se define la ubicación del nivel y severidad del riesgo dentro de la matriz de calor, la mayoría de los controles que se diseñan son para disminuir la probabilidad de que ocurra una causa o evento que pueda llevar a la materialización del riesgo.

Preventivos y Detectivos → PROBABILIDAD

Controles Correctivos → IMPACTO

Continuando con el ejemplo descrito en la guía y aplicando la tabla de atributos de los controles, se precisa:

Riesgo: Posibilidad de afectación jurídica, por uso de normativa desactualizada o derogada en la elaboración de conceptos jurídicos erróneamente fundamentados.

Probabilidad inherente = media 60%

Impacto inherente = mayor 80%

Zona de Riesgo = Alta.

f. Nivel del riesgo (riesgo Residual)

Es el resultado de aplicar la efectividad de los controles vs. los atributos al riesgo inherente, y se conoce como riesgo residual.

Empleando el resultado del ejemplo anterior en la tabla 6, se calcula el riesgo residual y su ubicación en la matriz de calor.

Tabla 6. Control vs. Atributos

Control	Característica			Peso
El funcionario del proceso gestión jurídica debe verificar y actualizar la normatividad al interior de la entidad y lo correspondiente a la jurisprudencia.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automática		
		Manual	X	15%
	Documentado	Documentado		
		Sin documentar	X	
	Frecuencia	Continua	X	
		Aleatoria		
	Evidencia	Con registro	X	
		Sin Registro		
Valoración control				**40%**

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 5. 48p.

- VC_1: Probabilidad 40%, Impacto 80%, Zona de riesgo Alta

Generando que la zona de calor inicial se conserve, sin embargo, el nivel de la probabilidad disminuya de acuerdo con la incidencia del control frente al riesgo.

Figura 11. Matriz de calor – Riesgo Residual

PROBABILIDAD	ZONA DE RIESGO				
MUY ALTA 100	ZONA DE RIESGO ALTA 2000	ZONA DE RIESGO ALTA 4000	ZONA DE RIESGO ALTA 6000	ZONA DE RIESGO ALTA 8000	ZONA DE RIESGO EXTREMA 10000
ALTA 80	ZONA DE RIESGO MODERADA 1600	ZONA DE RIESGO MODERADA 3200	ZONA DE RIESGO ALTA 4800	ZONA DE RIESGO ALTA 6400	ZONA DE RIESGO EXTREMA 8000
MEDIA 60	ZONA DE RIESGO MODERADA 1200	ZONA DE RIESGO MODERADA 2400	ZONA DE RIESGO MODERADA 3600	ZONA DE RIESGO ALTA 4800	ZONA DE RIESGO EXTREMA 6000
BAJA 40	ZONA DE RIESGO BAJA 800	ZONA DE RIESGO MODERADA 1600	ZONA DE RIESGO MODERADA 2400	ZONA DE RIESGO ALTA 3200	ZONA DE RIESGO EXTREMA 4000
MUY BAJA 20	ZONA DE RIESGO BAJA 400	ZONA DE RIESGO BAJA 800	ZONA DE RIESGO MODERADA 1200	ZONA DE ESGO ALTA 1600	ZONA DE RIESGO EXTREMA 2000
IMPACTO	20 INSIGNIFICANTE	40 MENOR	60 MODERADO	80 MAYOR	100 CATASTRÓFICO

Fuente: Elaborado por el Grupo de Planeación – Desarrollo Institucional de la DIGSA.

Nota: para la aplicación de los controles se debe tener en cuenta que la mitigación del riesgo sea de forma acumulativa, esto quiere decir que la valoración del control 2 se determinara tomando el valor el resultante de la valoración del control 1, aplicando la formula:

* $Probabilidad\ riesgo\ inherente\ (PRI)$
* $Valoración\ del\ control\ 1\ (VC_1)$
* $Valoración\ del\ control\ 2\ (VC_2)$

$$Fórmula\ valor\ de\ Probabilidad\ (VC_2): PRI - (PRI\ *\ VC_1)\ =\ VC_2$$

Ejemplo:

$$VC_2 = 60\% - (60\% * 40\%) = 36\%$$

g. Plan de Contingencia:

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

Aquellas actividades necesarias que contengan los planes de contingencia deberán contribuir para que se realice la investigación de la materialización y describir las

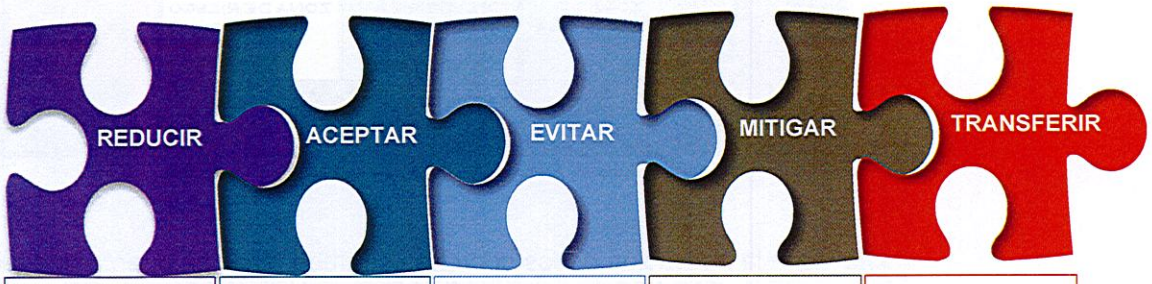
actividades requeridas para dar continuidad con las funciones y responsabilidades afectadas.

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

3.3. *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 evalúen las opciones existentes en materia de tratamiento del riesgo para la mitigación del riesgo, así como la relación costo-beneficio de las medidas de tratamiento, dicha decisión puede ser:

Figura 12. Estrategias para el manejo del riesgo



Adopta medidas para reducir la probabilidad o impacto, esto se determina mediante transferencia o mitigación.	No se adopta ninguna medida, se asume el mismo conociendo los efectos al materializarse.	Busca minimizar la probabilidad de materialización del riesgo.	Implementar acciones que mitiguen el nivel del riesgo, pueden estar asociadas al plan de acción*.	Reduce la probabilidad o el impacto, la mejor estrategia es tercerizar el proceso o trasladarlo a través de pólizas o seguros.

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

* 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 que permitan la correcta identificación, análisis, valoración y manejo de estos, siendo coherentes con los controles programados para los riesgos.

3.4. *Herramientas para la gestión del riesgo:*

Son elementos agregados que sirven de base para conocer si el riesgo fue identificado en algún momento y cuál fue su comportamiento, para ello se debe tener un histórico relacionado con:

Gestión de eventos - Base de Históricos:

1. PQRSF (peticiones, quejas, reclamos, sugerencias y felicitaciones).

2. Gestión jurídica.
3. Auditorias - Planes de mejoramientos.
4. Reportes de seguimiento.

Indicadores:

Captura la ocurrencia de un incidente asociado con el riesgo, generando reporte ocurrencias para el análisis de la eficacia de los controles.

3.5. *Monitoreo y Seguimiento*

En alineación con la dimensión 7 *"Control interno"* del Modelo Integrado de Planeación y Gestión – MIPG, se establece la responsabilidad y control, para la gestión del riesgo la cual es desarrollada por los funcionarios de la entidad.

a. Modelo de las líneas de defensa

Establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos[9] como se describe en la tabla 7.

Tabla 7. Líneas de Defensa, Rol y Responsabilidad

LÍNEA DE DEFENSA	ROL	RESPONSABILIDAD
Estratégica	•Alta Dirección •Subcomité Institucional de Coordinación de Control Interno.	Este nivel analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos, tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad.
1ª	•Líderes de proceso y sus equipos.	• La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. • La gestión operacional identifica, evalúa, controla y mitiga los riesgos
2ª	•Planeación estratégica •Líder de proceso •Gestor de proceso	• Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces. • Consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
3ª	•Oficina de Control Interno o quien haga sus veces. •Auditoría Interna	La función de la auditoría interna, a través de un enfoque basado en el riesgo, proporcionará aseguramiento objetivo e independiente 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.

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 5. 60p.

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

b. Responsable de Seguridad de la información[10]

- ✓ Actualizar por parte de la Dirección General de Sanidad Militar el procedimiento para la Identificación y Valoración de Activos de la Entidad, de con acuerdo a los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad).
- ✓ Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).
- ✓ Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
- ✓ 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 de la información.

c. Monitoreo

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 del riesgo, anexando sus debidas evidencias de acuerdo con lo establecido en los controles.

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

Tabla 8. Tiempos para el desarrollo del Monitoreo

TIPOLOGÍA	MONITOREO
Ejecución y administración de procesos Fraude externo Fallas tecnológicas Relaciones laborales Usuarios, productos y prácticas Daños a activos fijos/ eventos externos Seguridad de la información	Trimestral
Corrupción (Fraude interno)	Mensual

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

d. Seguimiento

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

[10] Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (Anexo 4 – DAFP) versión 2 Bogotá, Colombia 2019. 11p.

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:

a) Seguimiento: El jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles[11].

Seguimiento	Corte y Publicación
1 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.
2 seguimiento	Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
3 seguimiento	Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 5.

[11] 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. 73p.

ANEXOS

Formato Mapa de Riesgos Institucional DIGSA, bajo el código MDN-COGFM-PROPLAES-DIGSA-FU.95.1-43 en la plataforma Suite Visión Empresarial – SVE.

BIBLIOGRAFÍA

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

Departamento Administrativo de la Función Pública. (Versión 5 noviembre 2020). Guía para la Administración del Riesgo y el diseño de Controles en entidades Públicas.

Ministerio de Tecnologías de la Información y las Comunicaciones. (versión 2 agosto de 2019) Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (Anexo 4 – DAFP).

Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC. Norma Técnica Colombiana NTC ISO 31000:2018. Gestión del Riesgo. Principios y Directrices. Bogotá D.C.