"Por la cual se actualiza la Política de Administración de Riesgo de la Superintendencia de Vigilancia y Seguridad Privada".

EL SUPERINTENDENTE DE VIGILANCIA Y SEGURIDAD PRIVADA

En uso de sus atribuciones legales y en especial las que le confieren los 2355, 2356 de 2016 y demás normas concordantes.

CONSIDERANDO

Que de conformidad con lo establecido en el artículo primero de la Ley 87 del 29 de Noviembre de 1993, define el Control Interno como el sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una Entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos, así mismo en el artículo 2, literal (f) se establece que se deben definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.

Que la ley 1474 de 2011 o Estatuto Anticorrupción "…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"; que en su Artículo 73 señala que "Cada Entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano". Dentro de sus componentes se contempla el de "Gestión de riesgos", que incluye el mapa de riesgos de corrupción en la respectiva Entidad y las medidas concretas para mitigar los riesgos.

Que el gobierno nacional mediante el Decreto Nacional 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de la Función Pública", del cual fue sustituido el Titulo 22 mediante el Decreto Nacional 1499 de 2017, estableciendo el objeto e instancias de dirección y coordinación del Sistema de Gestión y adopta el Modelo Integrado de Planeación y Gestión –MIPG, definiéndolo como "un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las Entidades y organismos públicos. Este modelo opera a través de siete (7) dimensiones y (19) políticas de Gestión Institucional, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio". De acuerdo con la Dimensión "Direccionamiento Estratégico y Planeación" y el Plan Estratégico se formulan los objetivos y metas de largo plazo, para satisfacer las problemáticas y necesidades de los grupos de valor, identificando los posibles riesgos asociados al cumplimiento del plan institucional. Por lo tanto, la identificación y valoración de los riesgos se orienta a los objetivos de cada uno de los procesos.

Que según el artículo 2.2.21.1.6 del Decreto 648 de 2017 “Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública”, establece como una de las funciones del Comité Institucional de Coordinación de Control Interno la siguiente “Someter a aprobación del Representante Legal, la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta”.

En la Dimensión 2: Direccionamiento Estratégico y Planeación, establece que, desde la Alta Dirección, se deben emitir los lineamientos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.

En la Dimensión 7: Control Interno, determina la gestión de riegos en las Entidades del estado, bajo el liderazgo de la Alta Dirección y de todos los servidores de las Entidades, identificando, evaluando y gestionando los eventos que pueden afectar el cumplimiento de los objetivos, así como las actividades de control que permitan mitigar los riesgos hasta niveles aceptables.

Que, en el mes de junio de 2022, se emitió la Resolución N° 20221200039247 mediante la cual se actualizó la Política de Administración de Riesgo de la Superintendencia de Vigilancia y Seguridad Privada, la cual debe ser ajustada atendiendo a lo establecido en el Modelo Integrado de Planeación y Gestión - MIPG y la “Guía para la administración del riesgo y el diseño de controles en Entidades públicas - Versión 6 de noviembre de 2022”.

De conformidad con lo señalado, se presentó para aprobación la Política de Administración de Riesgo de la Superintendencia de vigilancia y seguridad privada, ante el Comité Institucional de Coordinación de Control Interno celebrado el 14 de agosto de 2023.

RESUELVE

ARTÍCULO 1. Introducción. La Superintendencia de Vigilancia y Seguridad Privada es un organismo del orden nacional, de carácter técnico, adscrito al Ministerio de Defensa Nacional, con autonomía administrativa y financiera. Le corresponde ejercer el control, inspección y vigilancia sobre la industria y los servicios de vigilancia y seguridad privada y con el propósito de revisar los lineamiento frente a la gestión de los riesgos, realiza la actualización de la Política de administración del Riesgo, teniendo en cuenta la actualización del Modelo Integrado de Planeación y Gestión- MIPG, versión 5 de marzo de 2023 y la metodología establecida en la Guía de administración del riesgo y el diseño de controles en Entidades públicas, versión 6 de 2022, siguiendo los tres pasos principales: 1. Política de administración de riesgos 2. Identificación del riesgo y 3. Valoración del riesgo.

Para la actualización de la política, se adoptarán las directrices del Modelo Integrado de Planeación y Gestión – MIPG y la metodología definida en la “Guía para la administración del riesgo y el diseño de Controles en Entidades públicas”, versión 6 del DAFP, para los riesgos de gestión, corrupción y Seguridad de la información. La política de administración de riesgos se define así:

"La Superintendencia de Vigilancia y Seguridad Privada, con el liderazgo de la Alta Dirección y la gestión de todos los servidores públicos, se compromete a identificar, valorar, controlar y administrar adecuadamente los riesgos de gestión y corrupción, de acuerdo con la metodología vigente; implementando los controles y las acciones oportunas para evitar la materialización y mantener niveles de riesgo aceptables".

ARTÍCULO 2. Objetivo. Establecer los lineamientos para la gestión de los riesgos en la Supervigilancia, con la definición de los criterios para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión, comunicación y consulta de los riesgos, que pueden afectar el cumplimiento de la misión y objetivos institucionales.

Objeticos Específicos:

- Determinar los niveles de aceptación del riesgo en la Entidad
- Definir las responsabilidades, atendiendo los roles establecidos en el esquema de las Líneas de Defensa para la Gestión de los riesgos.
- Establecer los lineamientos con relación a la definición de los planes de acción a partir del riesgo residual.

ARTÍCULO 3. Alcance. Los lineamientos de la Política de Administración del Riesgo serán aplicables a todos los procesos de la Entidad, con el propósito de gestionar los riesgos por parte de los servidores públicos y contratistas de acuerdo con las funciones, obligaciones, roles y responsabilidades.

ARTÍCULO 4. Glosario.
En el contexto de la gestión de riesgos, se relacionan los conceptos más importantes:

Activo de información: En términos de seguridad digital, hace referencia a las aplicaciones, información ya sea física o digital, servicios web, hardware, software y en general la información necesaria para la operación de las Entidades en el entorno digital.

Amenaza: Situación potencial de un incidente no deseado, que puede causar daño a un sistema o a una organización.

Apetito del Riesgo: Es el nivel de riesgo que la Entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la Entidad debe o desea gestionar.

Activo: En el contexto de seguridad digital hace referencia a elementos como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información TI, tecnologías de información TO, necesarias en las organizaciones para operar en el entorno digital (MinTic).

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Causa inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituye la causa principal para que se presente el riesgo.

Causa raíz: Es la casa principal o razones por las cuales se puede generar un riesgo.

CICCI: Comité Institucional de Coordinación de Control Interno

CGDI: Comité de Gestión y Desempeño Institucional

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

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

Control: Medida que permite reducir o mitigar un riesgo.

Gestión del riesgo: Proceso efectuado por la alta dirección de la Entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Factores de riesgo: Son las fuentes generadoras de riesgos

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

Integridad: En el contexto de la seguridad de la información, se refiere la información almacenada en los dispositivos o que siendo transmitida por los canales de comunicación no ha sido manipulada por terceros y no puede ser modificada por personas no autorizadas.

Mapa de riesgo: Documento con la información resultante de la gestión del riesgo.

MECI: Modelo Estándar de Control Interno

MIPG: Modelo Integrado de Planeación y Gestión

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

Plan Anticorrupción y de Atención al ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las Entidades.

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

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

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

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo de Fraude: La vulnerabilidad a la que está expuesta una organización cuando se combinan los elementos como presión, oportunidad y racionalización.

Fraude Interno: Perdida debido a actos de fraude, actuaciones irregulares, hechos delictivos, abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la Entidad, en las cuales está involucrado por lo menos un participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Fraude Externo: Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la Entidad).

Riesgo inherente: Nivel de riesgo propio de la actividad. Es el resultado de combinar la probabilidad con el impacto, permite determinar el riesgo inherente.

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

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

Vulnerabilidad: Es la representación de la debilidad de un activo o un control y que puede ser aprovechada por una o más amenazas.

ARTÍCULO 5. Responsabilidades

Según lo establecido en la Séptima Dimensión "Control Interno" del Modelo Integrado de Planeación y Gestión – MIPG, la responsabilidad para la gestión de los riesgos se define a través de las Líneas de Defensa.

LÍNEA ESTRATÉGICA
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento. A cargo de la alta dirección y el Comité Institucional de Coordinación de Control Interno.

1ra. LÍNEA DE DEFENSA	2da. LÍNEA DE DEFENSA	3ra. LÍNEA DE DEFENSA
Aplica y ejecuta procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. A cargo de los líderes de los procesos con el apoyo de sus colaboradores.	Monitorear la gestión del riesgo y control ejecutada por la primera línea de defensa. A cargo de: Jefe de Planeación, supervisores de contratos o proyectos, coordinadores, líderes de los sistemas de gestión de la Entidad, comité asesor de compras y adquisiciones	Proporciona un aseguramiento basado en la independencia y objetividad sobre la efectividad del Sistema de Control Interno. A cargo de la Oficina de Control Interno.

Fuente: Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES RELACIONADAS CON LA ADMINISTRACIÓN DE RIESGOS
LINEA ESTRATÉGICA	Comité Directivo/Comité Institucional Coordinación de Control Interno	- Establecer la Política de Administración del riesgo. - Revisar la exposición de la Entidad a los riesgos de corrupción y fraude. - Verificar y monitorear el cumplimiento de lo establecido en la Política de Administración de Riesgos. - Monitorear el estado de los riesgos aceptados (apetito del riesgo) e identificar los cambios que afecten el funcionamiento de la Entidad. - Analizar el resultado de las evaluaciones de la gestión de riesgos presentadas por la segunda y tercera línea de defensa.
PRIMERA LINEA	Todos los servidores y contratistas	-Identificar, valorar y definir la opción de tratamiento a los riesgos (de gestión, corrupción, seguridad digital, entre otros) que pueden afectar el logro de los objetivos de los procesos, programas o proyectos en los cuales participe, acorde con la Política de Administración del Riesgo. -Identificar cambios que incidan en los riesgos y proponer los ajustes correspondientes. -Identificar la posibilidad de fraude en los procesos, programas o proyectos en los cuales participe e informar oportunamente. -Revisar en coordinación con la segunda línea de defensa en la identificación de riesgos. - Definir y diseñar los controles (manuales o apoyados en TI) a los riesgos, según lo establecido en la metodología. -Establecer responsabilidades para la ejecución de las actividades de control y asegurar que personas competentes y con autoridad suficiente, efectúen dichas actividades con diligencia y oportunidad. -Elaborar los mapas de riesgo, que incluyan los riesgos de gestión, corrupción, entre otros. -Identificar cambios en los riesgos establecidos y proponer ajustes a los controles. -Efectuar monitoreo a los riesgos identificados y la aplicación de los controles de sus procesos, determinar y proponer posibles mejoras en los mismos.

SEGUNDA LÍNEA	Jefe Oficina Asesora de Planeación Supervisores de contratos o proyectos Coordinadores, líderes de los sistemas de gestión de la Entidad Comité asesor de compras y adquisiciones	- Evaluar y proponer modificaciones frente al diseño y desarrollo de la Política para la Gestión de Riesgos, con el fin de mantenerla actualizada. - Socializar la metodología de riesgos, líneas de defensa, objetivos, planes, programas y proyectos. - Liderar las mesas de trabajo para la actualización de los mapas de riesgos. - Verificar que el diseño y acciones de control se realice de acuerdo con la metodología vigente. -Identificar, socializar y publicar el mapa de riesgos de gestión y corrupción. -Consolidar el seguimiento a los mapas de riesgo y elaborar los informes consolidados. -Generar reportes periódicamente al Comité Institucional de Coordinación de Control Interno y al Comité de Gestión y Desempeño, acerca del cumplimiento de las metas y los objetivos con relación a la gestión integral del riesgo. - Revisar las exposiciones al riesgo alineado al contexto de los procesos. - Monitorear y evaluar el desarrollo de exposiciones al riesgo relacionadas con tecnología nueva y emergente. - Verificar que el diseño del control establecido por la primera línea de defensa sea pertinente frente a los riesgos identificados. – Verificar que los controles hayan sido ejecutados como han sido diseñados. - Implementar cultura de gestión de riesgos en la Entidad
TERCERA LINEA	Oficina de Control Interno	- Evaluar el cumplimiento de la Política de Administración de Riesgos en todos los niveles de la Entidad. - Evaluar que los mapas de riesgos se encuentren actualizados. - Evaluar y alertar oportunamente sobre cambios que afecten la exposición de la Entidad a los riesgos de corrupción y de fraude. - Evaluar que el diseño del control sea adecuado según la metodología frente a los riesgos identificados, así como la ejecución de los mismos. - Evaluar la efectividad de los controles.

Fuente: Elaboración propia

ARTÍCULO 6. Escenarios de riesgo que afectan la Continuidad del negocio

1. Crisis financiera
2. Actos de terrorismo
3. Desastre tecnológico
4. Ciberataques
5. Daños en la infraestructura física
6. Nuevas leyes o regulaciones
7. Pandemia

ARTÍCULO 7. Criterios para definir el nivel de probabilidad e impacto en los riesgos

La calificación del impacto para los Riesgos de Gestión, Corrupción y Seguridad Digital se definió de acuerdo con establecido en la "Guía para la administración del riesgo y el diseño de controles en Entidades públicas" – Versión 6.

Riesgos de gestión

Determinación de la probabilidad

La probabilidad de ocurrencia está asociada a la exposición del riesgo del proceso o actividad. Es así como la probabilidad inherente será el número de veces que pasa por el punto de riesgo en un periodo de un (1) año.

Criterios para definir la probabilidad

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

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas. Versión 6

Determinación del impacto

Según lo establecido en la "Guía de administración del riesgo y el diseño de controles en Entidades públicas" - Versión 6, se definen como variables principales los impacto económico y reputacional y en casos como: Afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnización a terceros, sanciones por incumplimiento de tipo legal, afectación de la imagen institucional por vulneración de la información y fallas en la prestación del servicio, son temas que tienen impacto económico y reputacional. Es así como cuando se presenten ambos impactos para un riesgo en diferentes niveles, se debe tomar el nivel más alto.

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

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas. Versión 6

Riesgos de Corrupción

En el marco del Plan Anticorrupción y de Atención al Ciudadano, establecido en la Ley 1474 de 2011, que define las estrategias los riesgos de corrupción y hacen parte del "Componente Gestión de Riesgos". Según lo definido en la "Guía para la administración del riesgo y el diseño de controles en Entidades públicas" - Versión 6. El riesgo de corrupción se define como la posibilidad de que, por acción u

omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Criterios para determinar el nivel de probabilidad

La probabilidad de ocurrencia está asociada a la exposición del riesgo del proceso o actividad. Es así como la probabilidad inherente será el número de veces que pasa por el punto de riesgo en el periodo de un (1) año.

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

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas. Versión 6

Determinación del impacto

Para los riesgos de corrupción, el análisis de *IMPACTO* se tendrá en cuenta únicamente los niveles “moderado”, “mayor” y “catastrófico”, no aplican los niveles de impacto “insignificante” y “menor”

Para definir estos niveles de impacto se deberán aplicar las siguientes preguntas, en el desarrollo de la elaboración de la matriz de riesgos para cada proceso:

No.	Pregunta: Si el riesgo de corrupción se materializa podría…	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la 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 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 e n el sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas – Versión 6

MEDICION DE IMPACTO RIESGOS DE CORRUPCION

Resolución No. 20231200058177

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Diana Marcela Medina Saavedra
Revisado para firma por	Malcolm Cuero Guarín - Oficina Asesora de Planeación Nicolás Arias Morales - Oficina Asesora Jurídica
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

DESCRIPTOR	DESCRIPCION	NIVEL	RESPUESTAS AFIRMATIVAS
MODERADO	Afectación parcial al proceso y a la dependencia. Genera medianas consecuencias para la Entidad.	5	1-5
MAYOR	Impacto negativo de la Entidad. Genera altas consecuencias para la Entidad.	10	6-11
CATASTROFICO	Consecuencias desastrosas sobre el sector. Genera consecuencias desastrosas para la Entidad.	20	12-19

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas – Versión 6

ARTICULO 8. Estructura para la valoración y descripción del control

La valoración de los controles está orientada a la medida que permite reducir o mitigar el riesgo. Los responsables de implementar y monitorear los controles son los líderes de proceso y sus equipos de trabajo.

La estructura que se propone para la descripción del control, siguiendo lo definido en la "Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas es la siguiente:

1. Responsable de ejecutar el control
2. Acción que se realiza
3. Complemento, en este se indican los detalles que identifican claramente el objeto del control.

Sin embargo, teniendo en cuenta lo anterior, esta descripción debe contener las seis (6) variables:

- Responsable
- Periodicidad
- Propósito
- Como se realiza
- Observación o desviación
- Evidencia.

ARTÍCULO 9. Nivel de aceptación del riesgo y tratamiento del riesgo

Tipo de riesgo	Zona de Riesgo Residual	Tratamiento
Riesgos de Gestión	Baja y Moderada	Cuando el riesgo se ubique en la zona *Baja y moderada*, este se *reduce* mediante el seguimiento y monitoreo de los controles existentes. De manera **CUATRIMESTRAL**, con el fin de asegurar que el nivel de riesgo se mantiene. Opcionalmente se pueden establecer acciones que no generen costos adicionales.
	Alta y Extrema	Se deben establecer acciones de control y **OBLIGATORIAMENTE**, plan de tratamiento de los riesgos con el fin de MITIGAR la probabilidad de ocurrencia y el impacto. Se debe realizar seguimiento y monitoreo **CUATRIMESTRAL.**
Riesgos de Corrupción *(No pueden ser aceptados en ningún nivel)*	Moderada/Alta y Extrema	Los riesgos de corrupción no serán aceptables en ninguno de los niveles en donde se ubiquen. Se deberán establecer las acciones de tratamiento que EVITEN su materialización. El seguimiento a los riesgos de corrupción se realizará de acuerdo con la normatividad vigente, en las fechas establecidas para el Plan Anticorrupción y de Atención al Ciudadano – PAAC. Con corte al 30 de abril/31 de agosto/31 de diciembre de cada vigencia.

Fuente: Elaboración propia

ARTÍCULO 10. Plan de acción para desarrollar la Política de Administración de Riesgos.

Se establece un plan de acción para el desarrollo de la Política de Administración de Riesgos en la Superintendencia de Vigilancia y Seguridad Privada:

No	ACTIVIDAD	PERIODICIDAD	PRODUCTO	RESPONSABLE
1	Actualizar y aprobar la política de administración de riesgos de la entidad, según la metodología vigente.	Una (1) vez al año	Política actualizada y aprobada	Oficina Asesora de Planeación. Alta dirección y Comité Institucional de Coordinación de Control Interno.
2	Actualizar el mapa de riesgos de gestión, corrupción de los procesos, de acuerdo con la metodología vigente.	Una (1) vez, durante el primer trimestre de la vigencia para actualizar los mapas de riesgo institucional por proceso. Así mismo de acuerdo con las autoevaluaciones del proceso cuando se requiera.	Mapa de riesgos actualizados por proceso.	Líderes de los procesos con sus equipos de trabajo. La Oficina Asesora de Planeación realizará apoyo y acompañamiento a los procesos.
3	Consolidar y publicar el mapa de riesgos institucional de la Entidad.	El mapa de riesgos consolidado se publicará durante el primer semestre de la vigencia.	Mapas de riesgos institucional publicado en la Página Web de la entidad.	Oficina Asesora de Planeación y Comunicaciones
4	Efectuar el monitoreo y seguimiento a la gestión de riesgos, así como al diseño y ejecución de controles de los riesgos de los procesos.	El monitoreo a los riesgos de gestión y corrupción se realizará con periodicidad semestral. Cada cuatro (4) meses se realizará seguimiento a los riesgos de corrupción y gestión (Los diez primeros días hábiles de los meses de mayo, septiembre y enero).		Oficina Asesora de Planeación. Oficina de Control Interno.

ARTÍCULO 11. Mapa de riesgos institucional

Le corresponde a la Oficina Asesora de Planeación consolidar el mapa de riesgos institucional.

ARTÍCULO 12. Actividades de Seguimiento y Monitoreo

La Oficina Asesora de Planeación realizará informe cuatrimestral de riesgos y ejecución de controles, con corte al 30 de abril, 31 de agosto y 31 de diciembre.

Adicionalmente, los Líderes de los procesos realizarán informe de evaluación semestral al desempeño de los procesos, que incluye la gestión realizada a los riesgos y controles de los riesgos de gestión y corrupción, así:

- Corte al 30 de junio y 30 de diciembre los líderes de los procesos comunican a la Oficina Asesora de Planeación la Evaluación al desempeño de los procesos, en el formato vigente FOR-SIG-121-026.
- La Oficina Asesora de Planeación realizará el informe semestral con los resultados consolidados, el cual se informará a los líderes de los procesos.

ARTÍCULO 13. Actividades de seguimiento y Evaluación

Según lo establecido en la Ley 87 de 1993, el artículo 73 de ley 1474 de 2011, el Decreto 1083 de 2015 y el Decreto 124 de 2016, el jefe de la Oficina de Control Interno o quien haga sus veces, debe adelantar seguimiento al Plan Anticorrupción y de Atención al Ciudadano, lo cual incluye los riesgos de corrupción:

- **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.

El seguimiento a los riesgos de corrupción, realizado por la Oficina de Control Interno se deberá publicar en el Línk de Transparencia de la página web de la Entidad, según los lineamientos establecidos.

Igualmente, para los riesgos de gestión, se debe realizar el informe de seguimiento y evaluación por parte de la Oficina Asesora de Planeación una vez al año finalizando la vigencia.

ARTICULO 14. Herramientas para la gestión de riesgo

Para la administración del riesgo en la Superintendencia de Vigilancia y Seguridad Privada, se siguen los lineamientos establecidos en la Política de Administración de Riesgos.

En el caso de materialización del riesgo y teniendo en cuenta los resultados del seguimiento, monitoreo y evaluación llevadas a cabo por los organismos de Control, entes de auditoria y líderes de procesos, estos últimos deberán establecer planes de mejoramiento, entendiéndose estos como el análisis de causas y los planes de acción que se realizan para minimizar o corregir los riesgos. Estos planes deberán ser remitidos a la Oficina Asesora de Planeación para su validación y cargue de los mismos en el aplicativo Suite Vision Empresarial.

ARTICULO 15. Divulgación

La Política de Administración del Riesgo se dará a conocer en todos los niveles de la Entidad, mediante canales formales y estrategias de comunicación existentes como son: correo institucional y en la Herramienta Suite Vision Empresarial.

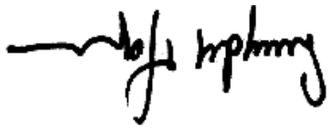
ARTICULO 16. Derogatoria

Esta Resolución deroga las disposiciones que sean contrarias.

ARTICULO 17. Vigencia

La presente Resolución rige a partir de la fecha de su publicación.

COMUNÍQUESE Y CÚMPLASE,



Fecha firma: 29/08/2023 16:29:20 GMT-05:00

ALFONSO MANZUR ARRIETA
Superintendente de Vigilancia y Seguridad Privada

Resolución No. 20231200058177

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Diana Marcela Medina Saavedra
Revisado para firma por	Malcolm Cuero Guarín - Oficina Asesora de Planeación Nicolás Arias Morales - Oficina Asesora Jurídica
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	