POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Decreto 1499 de 2017 establece los lineamientos para la implementación del Modelo Integrado de Planeación y Gestión, el cual es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas 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 del servicio.

La Gobernación de Santander traza la Política de Administración del Riesgo de acuerdo a los parámetros de la Dimensión de Direccionamiento Estratégico del Modelo Integrado de Planeación y Gestión, MIPG. La cual aplica a los procesos del Sistema Integrado de Gestión de la entidad el cual se encuentra alineado con Modelo Estándar de Control Interno, MECI, en lo que se refiere a las responsabilidades de las Línea Estratégica y Líneas de Defensa, los lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas formulados por el Departamento Administrativo de la Función Pública, DAFP, la cual articula los Riesgos de Gestión, Riesgos de Corrupción y Riesgos de Seguridad Digital.

La Política de Administración del Riesgo de la Gobernación de Santander resalta el grado de compromiso de la Entidad frente al cumplimiento de los Objetivos Estratégicos los cuales están alineados con los Objetivos de Desarrollo Sostenible ODS, direccionando a los procesos a asumir un pensamiento basado en riesgos, que permita anticiparse, disminuir y contrarrestar el impacto de eventos inesperados.

En la Política de Administración del Riesgo de la Gobernación de Santander, establece la metodología para la identificación, el análisis, la valoración, diseño de controles y el tratamiento de los riesgos que pudieran afectar el cumplimiento de su misión, así como la actuación preventiva, detectiva y correctiva para asumir, reducir y mitigar el riesgo e igualmente determina los planes de contingencia o acción, ante la materialización del riesgo.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer el marco general para la adecuada gestión de los riesgos y los potenciales escenarios de materialización de los mismos, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales mitigando las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales, disminuyendo las potenciales consecuencias negativas, reduciendo las vulnerabilidades ante las amenazas internas y externas o mejorando las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad.

2.2 OBJETIVOS ESPECÍFICOS

1. Establecer la metodología para la identificación, análisis y valoración de los Riesgos de Gestión, Seguridad Digital, sobre posibles actos de corrupción y otros ámbitos que se involucren, acorde con las directrices del Gobierno Nacional, de cada uno de los procesos que conforman el Sistema Integrado de Gestión de la Gobernación de Santander.
2. Establecer los niveles de aceptación, probabilidad e impacto y el tratamiento de los Riesgos de Gestión, Seguridad Digital y Corrupción de cada uno de los procesos que conforman el Sistema Integrado de Gestión de la Gobernación de Santander.
3. Establecer los roles y responsabilidades de las líneas de defensa de la Gobernación de Santander.
4. Alcanzar un nivel aceptable de riesgos residuales en todos los procesos, a través de la gestión de acciones de control, con el fin de asegurar el cumplimiento de la misión institucional, los compromisos de gobierno, los objetivos estratégicos y de procesos vigentes.
5. Gestionar de forma anticipada las vulnerabilidades o eventos que puedan afectar el logro de los objetivos institucionales desde el ámbito de la gestión, corrupción y seguridad digital.
6. Fomentar la cultura del autocontrol mediante las acciones preventivas y correctivas para la gestión del riesgo en todos los niveles de la Gobernación de Santander.

3. ALCANCE

La Política de Administración de Riesgo es aplicable a todos los procesos que conforman, el Sistema Integrado de Gestión de la Gobernación de Santander y a todas las actividades realizadas por los servidores públicos durante el ejercicio de sus funciones, contemplando un adecuado tratamiento de Riesgos de Gestión, Corrupción y Seguridad Digital, identificando sus factores generadores hasta el establecimiento de controles de tratamiento para los mismos.

4. MARCO NORMATIVO

NORMATIVIDAD	ARTICULO	CONTENIDO
Ley 87 de 1993	Artículo 2 Artículo 13	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). Artículos 2 OBJETIVOS DEL CONTROL INTERNO: literal 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 puedan afectar el logro de los objetivos.
Ley 489 de 1998	Capítulo VI	Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Referente al Sistema Nacional de Control Interno.
Ley 1474 de 2011	Artículo 8	Por el cual se dictan normas sobre el Sistema Nacional de control Interno de la Entidades y Organismos de la Administración Publica del Orden Nacional y territorial y se dictan otras disposiciones. (Modificado parcialmente por el Decreto 2593 del 2000 y por el Art .8 de la Ley 1474 de 2011)
Ley 1474 de 2011 Estatuto Anticorrupción	Artículo 73	Plan Anticorrupción y de Atención al Ciudadano: Señala la obligatoriedad para cada entidad del orden nacional, departamental y municipal de elaborar anualmente una estrategia de lucha contra la corrupción y las medidas para mitigar estos riesgos. Al Programa Presidencial de Modernización, Eficiencia, Transparencia, le corresponde diseñar la metodología para elaborar el Mapa de Riesgos de Corrupción.

NORMATIVIDAD	ARTICULO	CONTENIDO
Ley 1712 de 2014. Ley de transparencia y de acceso a la información pública	Artículo 18 y 19	Literal g) Deber de publicar en los sistemas de información del Estado o herramientas que lo sustituyan el Plan Anticorrupción y de Atención al Ciudadano.
Decreto 1499 de 2017	Numeral 2.2.1; 3.2.3	Manual operativo MIPG, 2019.

5. TERMINOS Y DEFINICIONES

Administración del Riesgo. Un 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 institucionales. (1)

Causa. Todos aquellos factores tanto internos como externos que solo o en combinación con otros, pueden producir la materialización de un riesgo.

Control. Medida que permite reducir o mitigar un riesgo.

Consecuencia. Los efectos o situaciones resultantes de la materialización del riesgo que impacta en los procesos, la entidad, los grupos de valor y demás partes Interesadas.

Amenazas. Causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización

Alta Dirección. personas que ocupa un cargo de elevada responsabilidad (mandato) en una organización o gobierno y participa en el ejercicio del poder (ya sea la suya o la de su superior o el empleador, público o privado legalmente), para la gobernación de Santander la alta dirección será el Gobernador y los Comités CIGD y CICCI

Establecimiento del contexto. Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo1.

CICCI. Comité Institucional de Coordinación de Control Interno.

Identificación del Riesgo. Proceso para encontrar, reconocer y describir el riesgo[2].

Líder o Responsable del proceso. Persona con la responsabilidad y autoridad para gestionar un riesgo.

[1] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN -ICONTEC. Norma Técnica Colombiana NTC-ISO31000. 2011. p. 20
[2] Ibid. p. 21

Mapa de Riesgos. Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos

Política. Directriz emitida por la dirección sobre lo que hay que hacer para efectuar el control.

Probabilidad. Probabilidad de ocurrencia del riesgo

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

Riesgo. Efecto que causa sobre los objetivos de la entidad, debido a eventos potenciales.

Riesgo Inherente. Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite identificar el nivel de riesgo inherente, dentro de unas escalas de severidad.

Auditoría Interna. Es un examen sistemático, objetivo e independiente de los procesos, actividades, operaciones y resultados de una Entidad Pública.

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

Riesgo de Corrupción. La posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular3.

Riesgos Seguridad Digital. Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas

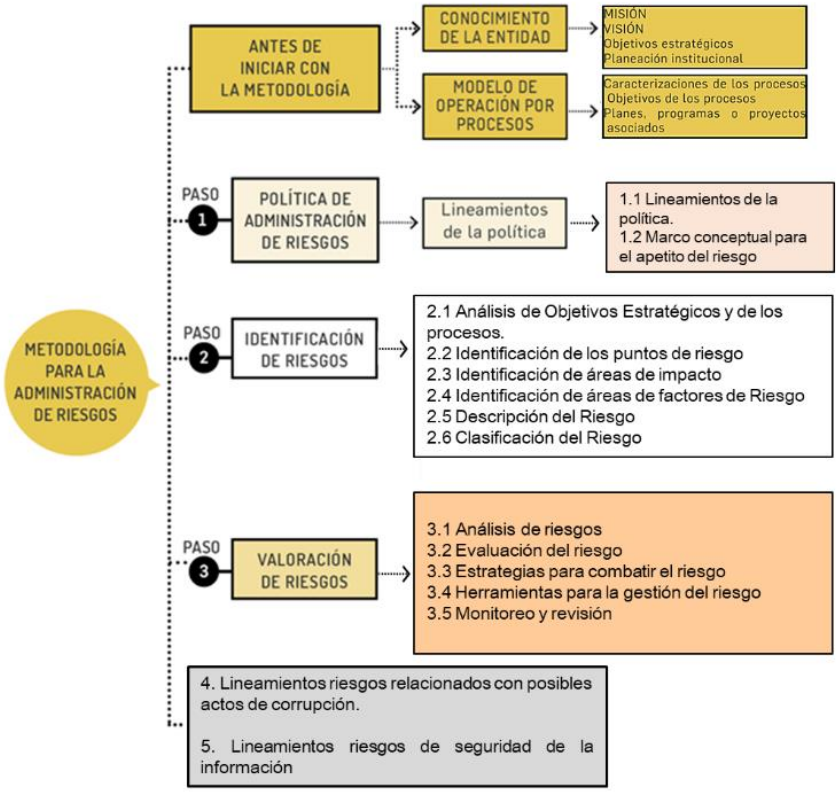
Factores de riesgo. Son las fuentes generadoras del riesgo.

Causa Raíz. Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.

6. METODOLOGÍA DE ADMINISTRACIÓN DEL RIESGO

La metodología para la administración del riesgo de la Gobernación de Santander se formula en concordancia con la propuesta por el Departamento Administrativo de la Función Pública; en virtud de esta idea se desarrolla el siguiente esquema que nos brinda la información más relevante en el proceso de la identificación de riesgos al que está expuesta la entidad.

[3] PRESIDENCIA DE LA REPÚBLICA/DEPARTAMENTO NACIONAL DE PLANEACIÓN/DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Estrategias para la construcción del plan anticorrupción y de atención al ciudadano. Bogotá. 2012. p.9



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

7. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

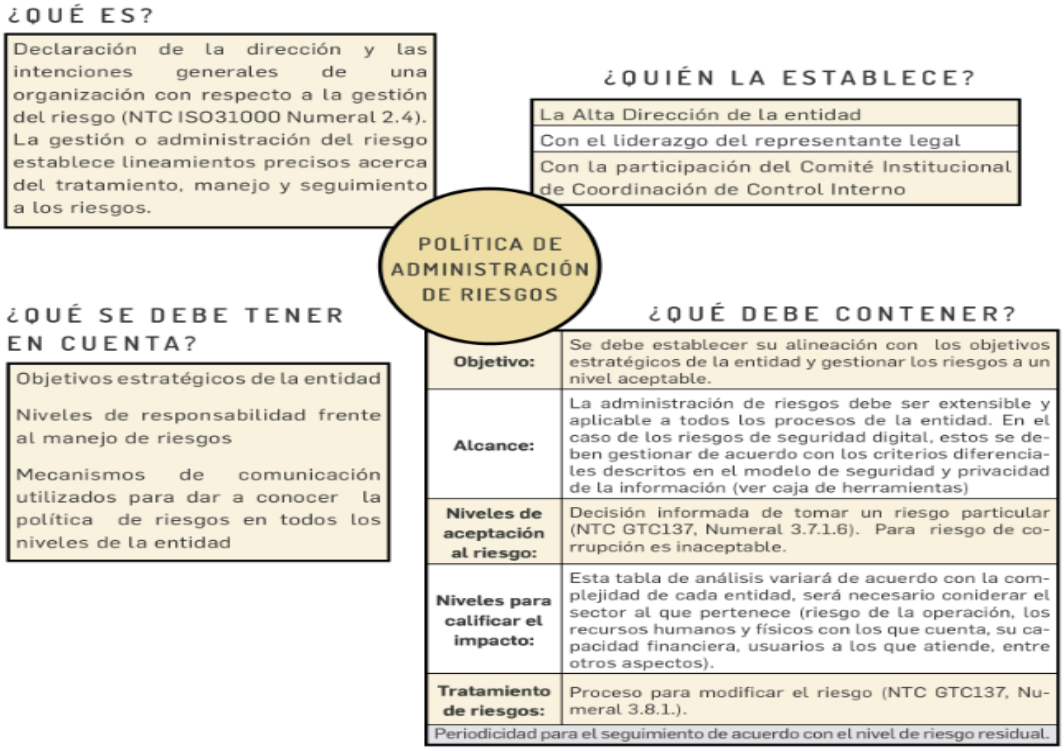
La política de administración de riesgos de la Gobernación de Santander, tiene un carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión, la guía de administración del riesgo y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad.

Las actividades relacionadas con la administración del riesgo de Gestión, Seguridad Digital y de Corrupción se revisarán cuatrimestralmente. La línea estratégica podrá determinar revisiones extraordinarias en aquellos casos en que se presenten cambios organizacionales o del entorno que puedan comprometer la gestión institucional.

La Dirección de Sistemas Integrados de Gestión, en cabeza de la Secretaria de Planeación, es la encargada de liderar la elaboración y consolidación de la matriz de riesgos por procesos, el mapa de Riesgos de Corrupción y Seguridad Digital.

La Oficina de Control Interno deberá presentar periódicamente un informe al Gobernador y a los responsables de los procesos respecto al estado de las acciones establecidas para mitigación de los riesgos identificados por Gestión, Corrupción y Seguridad Digital.

7.1. LINEAMIENTOS DE LA POLÍTICA



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

7.2. MARCO CONCEPTUAL PARA EL APETITO DEL RIESGO

Teniendo en cuenta que dentro de los lineamientos para la política de administración del riesgo se debe considerar el apetito del riesgo, a continuación, se desarrolla conceptualmente este tema.

- ✓ 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.
- ✓ Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- ✓ Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- ✓ Capacidad de riesgo: es el máximo valor del nivel 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.

7.3. IDENTIFICACIÓN DEL RIESGO – CONTEXTO DE LA GOBERNACION

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, teniendo en cuenta el contexto estratégico en el que opera la Gobernación de Santander, la caracterización de los procesos que conforman el Sistema Integrado de Gestión y que se encuentran alineados con el Modelo Integrado de Planeación y Gestión - MIPG, que contempla su objetivo y alcance, y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos. Para ello se contemplan los siguientes factores:

7.3.1 ANÁLISIS DEL CONTEXTO INTERNO

La Gobernación de Santander en su contexto interno determina las características o aspectos del ambiente interno como son su estructura organizacional, funciones y responsabilidades, políticas, objetivos, estrategias, recursos (económicos, personas, procesos, sistemas, tecnología, información), cultura organizacional para buscar el cumplimiento de los objetivos institucionales. Dentro del contexto interno se tendrán como factores principales:

CONTEXTO INTERNO	**FINANCIEROS:** presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

Identificación de los factores internos: Verificando los componentes de talento humano, direccionamiento estratégico que se hayan adelantado en la Institución se puede evidenciar y ocasionar la presencia de riesgos, hacen parte de estos factores internos todas aquellas fortalezas y debilidades que representan situaciones de riesgo para el logro de los objetivos de la entidad. Las situaciones internas están relacionadas con la estructura y la cultura organizacional, el modelo de operación, el cumplimiento de los planes, programas y proyectos, los sistemas de información, los procesos y procedimientos y los recursos humanos y económicos con los que cuenta la gobernación de Santander.

7.3.2 ANÁLISIS DEL CONTEXTO EXTERNO

Igualmente, en su contexto externo se determina las condiciones locales (nacionales e internacionales) que se interrelacionan con una nuestra entidad. Dentro del contexto externo se tendrán como factores principales:

CONTEXTO EXTERNO	**POLÍTICOS:** Cambios De Gobierno, Legislación, Políticas Públicas, Regulación.
	ECONÓMICOS Y FINANCIEROS: Disponibilidad De Capital, Liquidez, Mercados Financieros, Desempleo, Competencia.
	SOCIALES Y CULTURALES: Demografía, Responsabilidad Social, Orden Público.
	TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	AMBIENTALES: Emisiones y Residuos, Energía, Catástrofes Naturales, Desarrollo Sostenible.
	LEGALES Y REGLAMENTARIOS: Normatividad Externa (Leyes, Decretos, Ordenanzas y Acuerdos).

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

Identificación de los factores externos: Analizando la información externa, los planes, programas y proyectos se pueden identificar la presencia de riesgos en la Gobernación de Santander. Aquí se identifican circunstancias externas que puedan afectar el cumplimiento de los objetivos institucionales. Estas oportunidades y amenazas pueden ser tanto externas a la entidad como a cada proceso. Las situaciones del entorno pueden ser de carácter social, cultural, económico, tecnológico, político, ambiental y legal.

7.3.3 ANÁLISIS DEL CONTEXTO DE LOS PROCESOS

Igualmente, en su contexto del proceso se determina las condiciones de la estructura que permite mantener un control eficiente, efectivo de los procesos. Dentro del contexto de los Procesos se tendrán como factores principales:

CONTEXTO DE LOS PROCESOS	**DISEÑO DEL PROCESO:** Claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes
	TRANSVERSALIDAD: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	ACTIVOS DE SEGURIDAD DIGITAL DE LOS PROCESOS: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: Efectividad en los flujos de información determinados en la interacción de los procesos.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

La Gobernación de Santander para el análisis de los contextos expuestos cuenta con el formato (**ES-SIG-RG-13)** Contexto Estratégico de Riesgos, que consiste en una Matriz DOFA, que se debe diligenciar por los líderes de procesos y su equipo de trabajo. Este

documento permite la recolección de la información que se asocia a los riesgos a los que está expuesta la Gobernación:

7.3.4 IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

7.3.5. IDENTIFICACIÓN DE ÁREAS DE IMPACTO

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

7.3.6. IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Son las fuentes generadoras de riesgos. A continuación, se listan los factores de riesgo que puede tener la Gobernación de Santander.

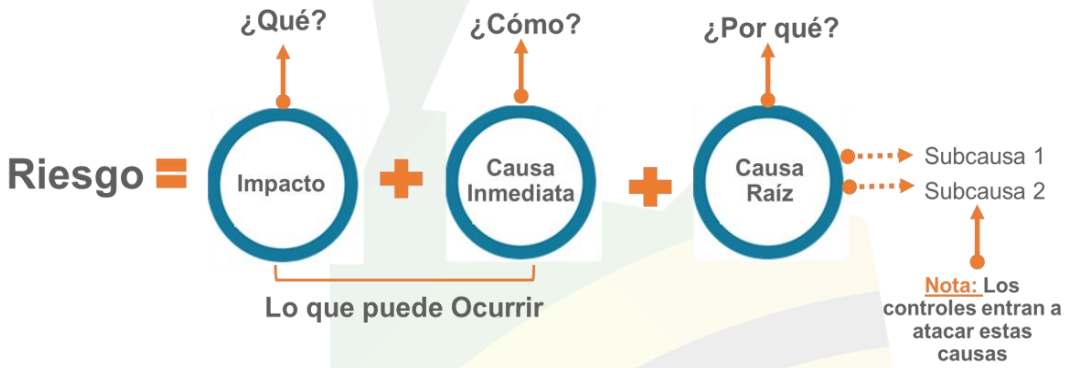
FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción	Hurto activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento Externo	Situaciones externas que afectan la entidad.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

7.3.7. DESCRIPCIÓN DEL RIESGO

La descripción del riesgo debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento, tanto para el líder del proceso en la Gobernación de Santander, como para personas ajenas al proceso.

Se propone una estructura que facilita su redacción y claridad se inicia con la frase **POSIBILIDAD DE** y se analizan los siguientes aspectos:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

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

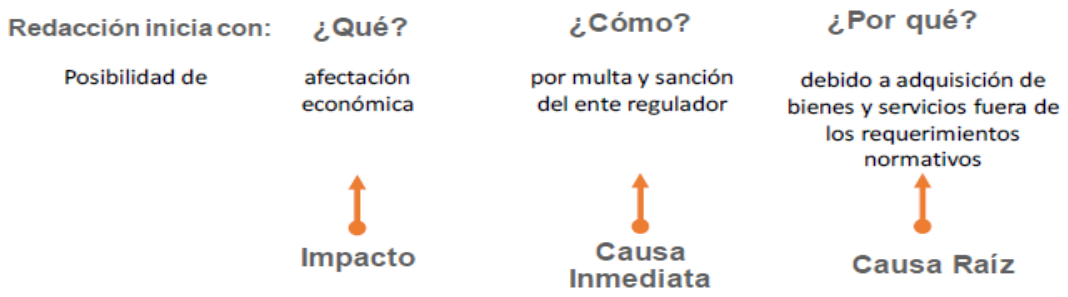
Causa Inmediata: Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o sub-causas que pueden ser analizadas.

Ejemplo para la redacción del riesgo

Proceso: gestión de recursos.
Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.
Alcance: inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisidores) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

7.4 CLASIFICACIÓN Y FACTORES DE LOS RIESGO

La clasificación del riesgo permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
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.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
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.
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.
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.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

Teniendo en cuenta lo anterior se definió una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

7.5 VALORACIÓN DEL RIESGO

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial, riesgo inherente. Los elementos que lo desarrollan son los siguientes:

7.5.1. ANÁLISIS DE LOS RIESGOS.

Busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial, riesgo inherente.

Nivel Probabilidad para Riesgos de Gestión, Seguridad Digital y Corrupción.

El nivel de probabilidad estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando en la Gobernación de Santander, es decir el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la siguiente tabla se establecen los criterios para definir el nivel de 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 5, DAFP

Nivel de Impacto para Riesgos de Gestión y Seguridad Digital.

El nivel de impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo. Para evaluarlo en los riesgos de gestión y seguridad digital se deberá tener en cuenta la siguiente tabla:

	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 5, DAFP

Nivel de Impacto para Riesgos de Corrupción

Para la evaluación del nivel de impacto de los riesgos de corrupción se deberá responder las siguientes preguntas:

PREGUNTAS	RESPUESTA	
	SI	NO
1. ¿Afectar al grupo de funcionarios del proceso?		
2. ¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3. ¿Afecta 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. ¿Genera 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. ¿Genera perdida 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?		

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

De acuerdo a las respuestas afirmativas se clasifica el impacto como se observa en la siguiente tabla:

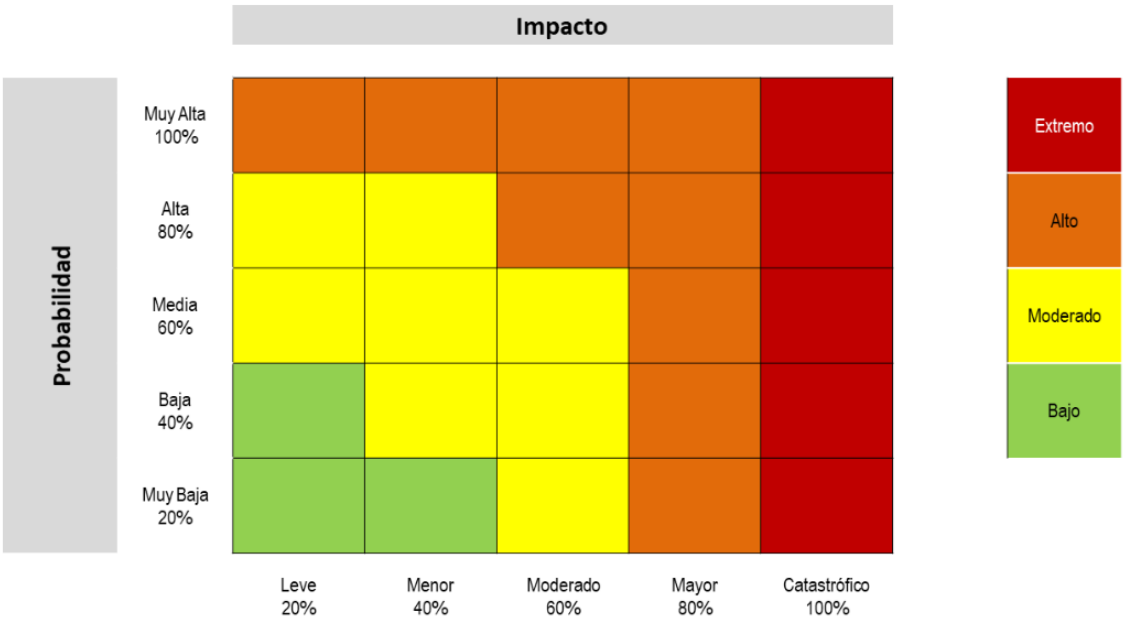
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

NIVEL - PREGUNTAS	DESCRIPTOR	DESCRIPCIÓN
1 a 5	Moderado	Afectación parcial al proceso y a la dependencia Genera medianas consecuencias para la entidad.
6 a 11	Mayor	Impacto negativo de la Entidad Genera altas consecuencias para la entidad.
12 a 19	Catastrófico	Consecuencias desastrosas sobre el sector Genera consecuencias desastrosas para la entidad.

7.5.2. EVALUACIÓN DE LOS RIESGOS

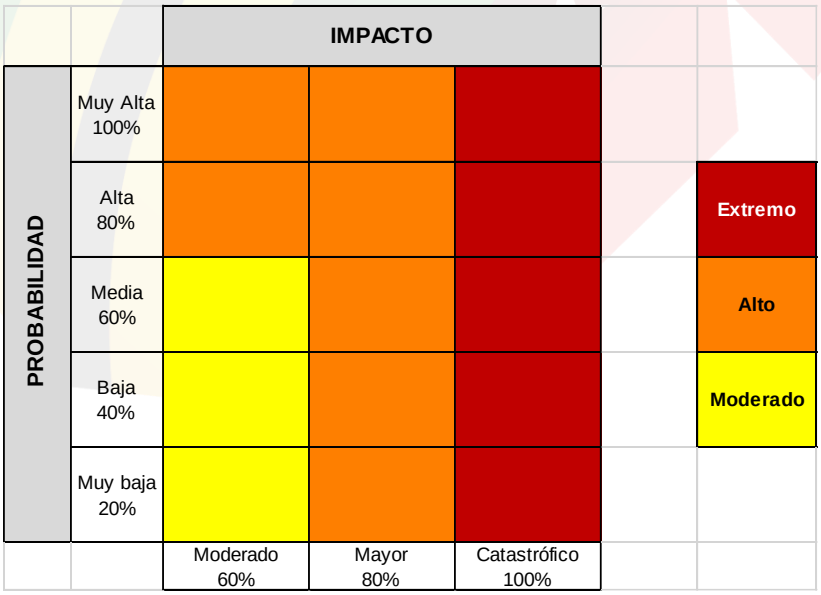
A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial llamado Riesgo Inherente.

Análisis preliminar (riesgo inherente) para riesgos de gestión y de seguridad digital: Se trata de determinar los niveles de severidad, a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor como se puede observar en la gráfica a continuación:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

Análisis preliminar (riesgo inherente) para riesgos de corrupción: Para los riesgos de corrupción, se realizará teniendo en cuenta solamente los niveles moderado, alto y catastrófico, dado que estos riesgos siempre serán significativos.

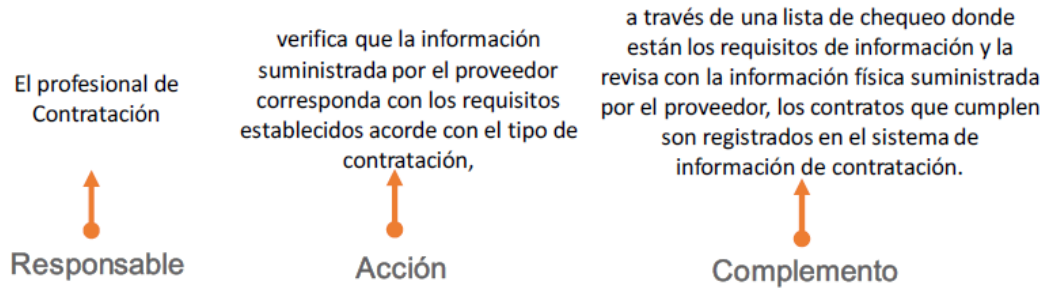


8 ESTRUCTURA DE LOS CONTROLES

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

1. **Responsable de ejecutar el control:** Identifica el cargo del servidor que ejecuta el control, en caso se ser controles automáticos se identificará el sistema que realiza la actividad.
2. **Acción:** Se determina mediante verbos en los cuales se identifica la acción a realizar como parte del control.
3. **Complemento:** Corresponde a los detalles que permiten identificar claramente el objeto del control. (Responsable, Periodicidad, propósito, controles, evidencias).

Ejemplo:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

8.1 TIPOS DE CONTROLES

Acorde con lo anterior tenemos las siguientes tipologías de controles:

Control Preventivo: Acción y/o mecanismo ejecutado antes que se realice la actividad originadora del riesgo, se busca establecer condiciones que aseguren el resultado final esperado. En general estos controles actúan sobre las causas del riesgo.

Control Detectivo: Acción y/o mecanismo ejecutado que permite detectar el riesgo durante la ejecución del proceso y puede disminuir la materialización de dicho riesgo. Estos controles detectan el riesgo, pero genera reprocesos.

Control Correctivo: Acción que se ejecutan después de que se materializa el riesgo y en la mayoría de ocasiones permiten reducir el impacto de dicho riesgo.

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

Control Manual: Controles que son ejecutados por una persona, tiene implícito el error humano

Control 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.

8.2 ANÁLISIS Y VALORACIÓN DE LOS CONTROLES

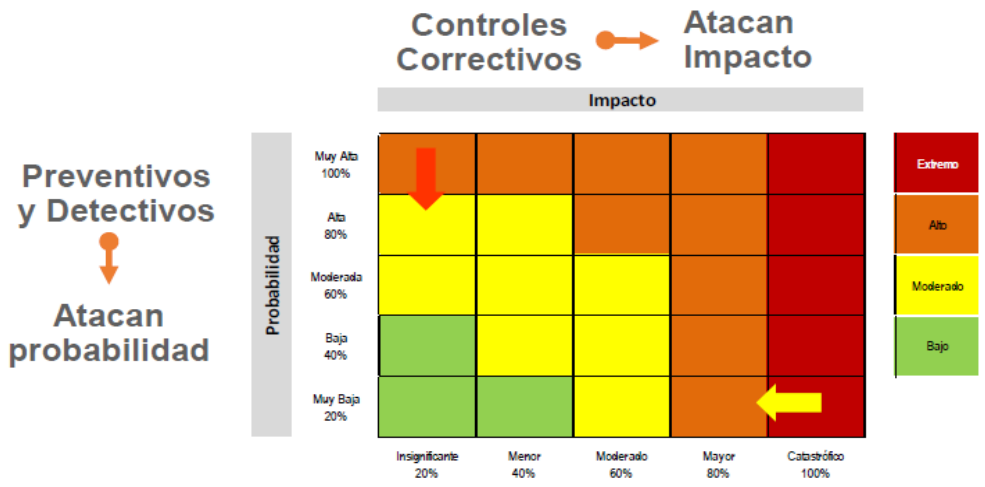
Los controles definidos de acuerdo con sus atributos influyen en la valoración del riesgo inherente teniendo en cuenta las siguientes condiciones:

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso..	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del	-

Características			Descripción	Peso
			riesgo.	
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del 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, DAFP

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde de la figura a continuación se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

Ejemplo:

En la tabla continuación se observa la aplicación de la tabla de atributos, esta servirá como ejemplo para el análisis y valoración de los controles propuestos.

CONTROL	CARACTERÍSTICAS			PESO
El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	TIPO	PREVENTIVO	X	25%
		DETECTIVO		
		CORRECTIVO		
	IMPLEMENTACIÓN	AUTOMÁTICO		
		MANUAL	X	15%
	DOCUMENTACIÓN	DOCUMENTADO	X	N.A.
		SIN DOCUMENTAR		
	FRECUENCIA	CONTINUA	X	N.A.
		ALEATORIA		
	EVIDENCIA	CON REGISTRO	X	N.A.
		SIN REGISTRO		
TOTAL VALORACIÓN CONTROL 1				**40%**
CONTROL	**CARACTERÍSTICAS**			**PESO**
El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	TIPO	PREVENTIVO		
		DETECTIVO	X	15%
		CORRECTIVO		
	IMPLEMENTACIÓN	AUTOMÁTICO		
		MANUAL	X	15%
	DOCUMENTACIÓN	DOCUMENTADO	X	N.A.
		SIN DOCUMENTAR		
	FRECUENCIA	CONTINUA	X	N.A.
		ALEATORIA		
	EVIDENCIA	CON REGISTRO	X	N.A.
		SIN REGISTRO		
TOTAL VALORACIÓN CONTROL 2				**30%**

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

8.3 RIESGO RESIDUAL

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

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2º control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2 %**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP

Así las cosas, se concluye que:

8.4. ESTRATEGIAS PARA TRATAR EL RIESGO

Es la respuesta establecida por la Primer Línea de Defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de Corrupción. Entre estas se encuentran:

- ✓ **Aceptar el Riesgo:** Después de un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.
- ✓ **Reducir el Riesgo:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.
- ✓ **Evitar el Riesgo:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

Transferir el Riesgo: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

Mitigar el riesgo: Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

Los líderes de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo, derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. Para los riesgos identificados en los procesos de la Gobernación de Santander se deberán tener en cuenta los siguientes parámetros:

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
Riesgos de Gestión y de Seguridad Digital	Baja	Se ***ACEPTA*** el riesgo y se administra por medio de las actividades propias del proceso, igual debe existir un seguimiento continuo del riesgo.
	Moderada	Se establecen acciones de control preventivas que permitan ***REDUCIR***, la probabilidad e impacto de ocurrencia de este riesgo
	Alta y Extrema	Se puede optar por un Plan de Acción, Acción Preventiva o cambio de controles para reducir, evitar y compartir la ocurrencia y consecuencia del riesgo.
Riesgos de Corrupción	Baja	Ningún riesgo de corrupción podrá ser aceptado
	Moderada	Ningún riesgo de corrupción podrá ser aceptado, implementar controles para reducir, evitar y compartir
	Alta y Extrema	Ningún riesgo de corrupción podrá ser aceptado implementar controles para reducir, evitar y compartir

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

9 ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DE LOS RIESGOS

TIPO DE RIESGO	RESPONSABLE	ACCIÓN
Riesgos de Gestión y de Seguridad Digital	Líderes de los Procesos	Revisar y reportar a planeación, el estado de operación de los controles, evitando incumplimientos de los procesos y los eventos e los que se han materializado los riesgos en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a estos 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. Revisar la planeación inicial antes de la materialización del riesgo y ajustar el diseño de los controles, volver a identificar riesgos y ejecutar el plan de acción evitando la materialización del riesgo.
	Secretaria de Planeación – Secretaría TIC	Revisar la implementación y asesorar la gestión del riesgo en los procesos verificando la adecuada identificación, análisis, valoración, monitoreo y revisión de riesgos, fortalezas en el diseño y ejecución de controles. Adelantar monitoreo a los controles implementados en la primera línea de defensa y evaluar su cumplimiento, así como asesorar en caso de materialización de los riesgos la ejecución de los planes de acción.
	Control Interno	Hacer seguimiento a que las actividades de control establecidas por los procesos para la mitigación de riesgos y los planes de acción establecidos como resultados de auditoria se realicen de manera oportuna cerrando la causa raíz del problema evitando en lo posible la repetición de hallazgos o materialización de riesgos. Revisar que se hayan identificado riesgos significativos que afectan el cumplimiento de los objetivos de los procesos incluyendo los de corrupción, adecuado diseño y ejecución de controles y que la calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. Realizar recomendaciones y seguimiento para el fortalecimiento de los controles.
Riesgos de Corrupción	Líder del Proceso	Informar a la línea estratégica el hecho encontrado. Realizar la respectiva denuncia ante la instancia de control pertinente.

TIPO DE RIESGO	RESPONSABLE	ACCIÓN
		Identificar las acciones correctivas necesarias y documentarlas en un plan de mejoramiento. Actualizar mapa de riesgos.
	Planeación	Informar al líder del proceso, quien analizará la situación y definirá las acciones a quien haya lugar. Dar lineamientos para que se implementen las acciones correspondientes, con el líder del proceso para la revisión y ajuste del mapa de riesgos. Informar a la alta gerencia de la materialización del riesgo.
	Oficina de Control Interno	Informar al líder del proceso, quien analizará la situación y definirá las acciones a quien haya lugar Realizar la respectiva denuncia ante la instancia de control pertinente Informar a la segunda línea de defensa con el fin de dar inicio a las acciones correspondientes, con el líder del proceso para la revisión y ajuste del mapa de riesgos.

10 RESPONSABILIDAD Y COMPROMISOS FRENTE A LA POLITICA DE ADMINISTRACION DEL RIESGO

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDAD FRENTE AL RIESGO
Estratégica	Alta Dirección	**1.** Revisar los cambios en el direccionamiento estratégico y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. 2. Analizar los cambios en el entorno (Contexto Interno y Externo), que puedan tener un impacto significativo en la operación de la entidad. 3. Realimentar al CIGD, CICCI sobre los ajustes que se deban hacer en la entidad sobre la Gestión del Riesgo en la entidad (Cuatrimestral, antes de adelantarse el comité de coordinación de control interno). 4. Hacer seguimiento y pronunciarse por lo menos cada cuatrimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas.

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDAD FRENTE AL RIESGO
		5. Revisar los informes presentados por lo menos cada cuatrimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, 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. 6. Revisar los planes de acción 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	Líderes de los procesos	1. Identificar y valorar los riesgos que puedan afectar los objetivos de su proceso a cargo, y hacer una actualización continua del mismo. 2. Definir, aplicar y realizar mejoramiento continuo, a los controles para mitigar los riesgos identificados, alineados con las metas y objetivos de la entidad. 3. Proponer mejoras a la gestión del riesgo de su proceso. 4. Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar la deficiencia de los controles y determinar las acciones de mejora que haya lugar. 5. Informar cuatrimestralmente a la Secretaría de Planeación (Segunda Línea), sobre los riesgos materializados en los planes y procesos a su cargo. 6. Reportar a la Secretaría de Planeación, los avances y evidencias de la gestión del riesgo a cargo de su proceso asociado.
Segunda Línea	Secretaría de Planeación	1. Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. 2. Presentar al Comité Institucional de Coordinación de Control Interno (CICCI), el monitoreo a la eficacia de los controles. 3. Asesorar y Supervisar que la primera línea identifique, evalué y gestione los riesgos y

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDAD FRENTE AL RIESGO
		controles, para que se efectúen acciones de mejora. 4. Identificar cambios en los niveles de aceptación del riesgo en la entidad, especialmente de los riesgos ubicados en zona baja y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno (CICCI) 5. Monitorear de forma cuatrimestral, los riesgos de corrupción, gestión y seguridad digital, identificados y los controles establecidos, por la primera línea de defensa 6. Evaluar conjuntamente con la primera línea de defensa, que los riesgos sean consistentes, con la presente política 7. Aprobar a través de la Dirección de Sistemas Integrados de Gestión, las acciones de mejora propuestas por los líderes de los procesos 8. Asesorar, orientar y capacitar a los líderes de los procesos, en identificación, análisis y valoración del riesgo y definición de controles 9. Garantizar capacitación a los líderes de procesos en la metodología de implementación de gestión del riesgo
	Secretaría TIC	1. Asesorar a la primera línea en la identificación y valoración de los riesgos de seguridad digital que puedan afectar los objetivos de sus procesos a cargo. 2. Asesorar a la primera línea en la definición y aplicación de controles que buscan mitigar los riesgos de seguridad digital identificados. 3. Apoyar a la secretaría de planeación en el monitoreo de los riesgos de seguridad digital identificados y los controles establecidos por la primera línea. 4. Apoyar a la Secretaría de planeación en la evaluación conjuntamente con la primera línea de defensa, de los riesgos identificados en los mapas de riesgo. 5. Monitorear de forma cuatrimestral, los riesgos de corrupción, gestión y seguridad digital, identificados y los controles establecidos, por la primera línea de defensa.
Tercera Línea	Oficina de Control Interno	1. Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y los controles,

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDAD FRENTE AL RIESGO
		con énfasis en el diseño e idoneidad de los controles establecidos por los procesos 2. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa 3. Llevar a cabo el seguimiento de a los riesgos consolidados en los mapas de riesgos y reportar los resultados al Comité Institucional de Coordinación de Control Interno (CICCI) 4. Recomendar mejoras a la política de administración del riesgo

11 PERIODICIDAD DEL MONITOREO Y SEGUIMIENTO

Con el fin de lograr un esquema articulado de comunicación entre las líneas de defensa para el monitoreo y seguimiento a los riesgos se establecen los siguientes periodos para realizarlo de acuerdo a las responsabilidades y competencias en el Sistema de Control Interno, así:

Monitoreo riesgos de Corrupción, Seguridad Digital y Gestión: El monitoreo se realiza cuatrimestralmente por la Secretaría de Planeación/Dirección de Sistemas Integrados de Gestión a todos los procesos tres (3) veces al año, de acuerdo a la información presentada por las líneas de defensa, en las siguientes fechas:

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

Seguimiento riesgos de Corrupción, Seguridad Digital y Gestión: El seguimiento se realiza cuatrimestralmente por la oficina de Control Interno a todos los procesos tres (3) veces al año, de acuerdo a la información presentada por las líneas de defensa, en las siguientes fechas:

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

El seguimiento adelantado por la oficina de Control Interno, se deberá publicar en la página web de la entidad o en lugar de fácil acceso al ciudadano.

12 DIVULGACIÓN O PUBLICACIÓN DE LA POLÍTICA

La Política de Administración de Riesgos deberá ser divulgada oficialmente a todos los servidores públicos y contratistas que prestan sus servicios en la Gobernación de Santander. De igual manera deberá ser incorporada y explicada en los procesos de inducción y reinducción efectuados por la entidad al momento de la vinculación de los servidores públicos y contratistas que prestaran sus servicios a la entidad.

La publicación de la política será efectuada en el enlace de Transparencia y Acceso a la Información Pública ubicado en la sede electrónica de la Gobernación de Santander.

13. EVALUACIÓN DE LOS CONTROLES

En el proceso de monitoreo realizado por la segunda línea de defensa se debe evaluar el adecuado diseño de los controles; por lo tanto, se deberán tener en cuenta las siguientes variables:

VARIABLES A EVALUAR Y ANALIZAR PARA EL ADECUADO DISEÑO DE LOS CONTROLES	
PASOS	**DESCRIPCION**
1. Responsable	Debe tener definido el responsable de llevar a cabo la actividad de control.
2. Periodicidad	Debe tener una periodicidad definida para su ejecución.
3. Propósito	Debe indicar cuál es el propósito del control.
4. Cómo se realiza la actividad de control	Debe establecer el cómo se realiza la actividad de control.
5. Qué pasa con las observaciones o desviaciones	Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control
6. Evidencia de la ejecución del control	Debe dejar evidencia de la ejecución del control.

En la tabla que se muestra a continuación puede observar el propósito, desviación, descripción y peso asociados, así mismo de identifican los atributos de formalización, que se recogerán de manera informativa, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos éstos no tienen una incidencia directa en su efectividad.

CRITERIO DE EVALUACIÓN.	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1.1 Asignación del responsable	Asignado	15
	No Asignado	0
1.2 Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

13.1. Resultados de la evaluación del diseño del control

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado

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

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