# **INTRODUCCIÓN**

La Gobernación del Huila como ente coordinador y articulador del desarrollo sostenible del Departamento, está comprometida con la política de operación para la administración de riesgos que pudieran afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos, planes institucionales, la satisfacción de los usuarios y el manejo transparente de los recursos públicos, a partir de la elaboración y adopción de la presente política de operación y la herramienta de trabajo, documentos técnicos que facilitan la buena “Gestión y Administración de los riesgos de gestión, corrupción y seguridad digital”, a través de los cuales se establecieron los lineamientos para la identificación, valoración, Diseño y ejecución de controles, tratamiento y seguimiento de dichos riesgos, tomando como referentes las directrices establecidas por el Departamento Administrativo de la Función Pública -DAFP y del Modelo Integrado de Planeación y Gestión – MIPG, conforme a la política de “Direccionamiento estratégico y planeación”, de “Definir la política de administración de riesgos, identificar y valorar riesgos (operativos, corrupción, contratación y defensa jurídica), de acuerdo con la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI, la Guía para la Administración del riesgo del DAFP, el Modelo de Seguridad y Privacidad de la información de la estrategia de Gobierno Digital y la Secretaría de Transparencia de la Presidencia de la República desde su estrategia Plan Anticorrupción y de Atención al Ciudadano.

En tal sentido, la Gobernación del Huila actualizará anualmente sus mapas de Riesgos de gestión, corrupción y seguridad digital, con el fin de ajustar controles y mitigar los riesgos en el marco de la viabilidad jurídica, técnica, financiera y económica. Los responsables de cada proceso, junto con sus equipos de trabajo, serán quienes adelanten la ejecución de los controles y las acciones preventivas y realicen el seguimiento a su cumplimiento como primera línea de defensa y mecanismo de autocontrol, conforme lo establece el Esquema de asignación de responsabilidades establecido.

Estos lineamientos, deben ser acatados por todos los servidores públicos y contratistas de la entidad en el desarrollo de sus funciones, compromisos y obligaciones, buscando que éstos conduzcan a disminuir la vulnerabilidad frente a las diferentes situaciones que puedan interferir en el logro de la misionalidad y objetivos institucionales y preparar la respuesta oportuna a amenazas externas que puedan generar eventos de riesgo, para lo cual se establecen las siguientes etapas:

1. Objetivos
2. Alcance
3. Esquema de asignación de responsabilidades
4. Metodología General para la administración de los riesgos de corrupción, gestión y seguridad digital
	1. Identificación de Riesgos
	2. Valoración de Riesgos
	3. Diseño y ejecución de controles
	4. Tratamiento y seguimiento

# **OBJETIVO**

**2.1. GENERAL**.

Establecer criterios metodológicos unificados, estandarizados y el marco general de actuación para la implementación de la política de administración de los riesgos de gestión, corrupción y Seguridad digital de la Gobernación del Huila, fortaleciendo el enfoque preventivo que conduzca a disminuir la vulnerabilidad frente a eventos internos o externos, que pueden afectar o impedir el logro de los objetivos institucionales y estratégicos, determinando los roles y responsabilidades de cada uno de los servidores de la entidad con base en el Esquema de las líneas de defensa, para una buena administración, tratamiento, divulgación y monitoreo de los mismos.

**2.2. ESPECÍFICOS.**

Identificar, priorizar y monitorear los riesgos de gestión, corrupción y seguridad digital, a partir de los factores críticos de éxito para que los directivos definan las principales directrices para implementación de los controles del proceso, contribuyendo y garantizando el normal desarrollo y cumplimiento de los objetivos del proceso y logro de los objetivos estratégicos de la entidad.

Valorar los riesgos como mínimo 1 vez al año, para que se evalúe el nivel de criticidad de los riesgos y determinar la política de tratamiento, conforme al nivel del riesgo residual.

Tratar mediante planes de mejoramiento y/o tratamiento, con enfoque preventivo y eficaz, para mitigar los riesgos y mejorar el desempeño institucional, conforme a la política de aquellos riesgos residuales, ubicados en la zona moderada, alta y extrema

Efectuar seguimiento mensual a todos los riesgos de corrupción que se encuentren en cualquier zona de riesgo, y a los riesgos de Gestión y seguridad digital ubicados en la zona moderada, alta y extrema, incluyendo la aplicación de controles para evitar la materialización.

# **ALCANCE**

# Esta política aplica para los riesgos de gestión, corrupción y seguridad digital, conforme a la estructura de procesos de la Gobernación del Huila. Es decir, aplica para todos los procesos de la entidad.

# La presente política, recoge las diferentes versiones de documentos que vienen dando directrices en materia de riesgos de gestión y corrupción, y se modifica con ocasión de la entrada en vigencia del Modelo Integrado de Planeación y Gestión (MIPG), que integra los Sistemas de Gestión de la Calidad y de Desarrollo Administrativo, crea un único Sistema de Gestión y, lo articula con el Sistema de Control Interno, el cual se actualiza y alinea con los mejores estándares internacionales, como son el Modelo COSO 2013, COSO ERM 2017 y el Modelo de las Tres Líneas de Defensa, con el fin de entregar a los ciudadanos, lo mejor de la gestión para producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción, conforme a la “Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital” versión 4 expedida por el Departamento Administrativo de la Función Pública de octubre de 2018.

# **LINEAS DE DEFENSA**

**Asignar las responsabilidades para cada componente en la gestión de riesgos**

El esquema de asignación de responsabilidades, adaptada del Modelo “Líneas de Defensa”, el cual puede apreciarse en la siguiente gráfica:



El anterior esquema de asignación de responsabilidades, para la gestión de riesgos en la Gobernación del Huila, queda, así, conforme a las tres líneas de defensa:

|  |  |  |  |
| --- | --- | --- | --- |
| **Líneas de Defensa** | **1º. Línea de Defensa** | **2º. Línea de Defensa** | **3º. Línea de Defensa** |
| Gestión del Riesgo | Responsables, Líderes y colaboradores de procesos - Servidores públicos la entidad | Secretaría General – Coordinador Sistema de Gestión | Oficina de Control interno |
| Factores claves de éxito de los procesos de la entidad | IdentificanValoranTratamiento y seguimiento | Responde a la línea estratégica: diseña herramientas de aplicación, acompaña proceso de aplicación | Asesora, recomienda, realiza auditoría independiente |

Responsabilidades:

|  |  |  |
| --- | --- | --- |
| **Líneas deDefensa** | **Responsable** | **Responsabilidad frente al riesgo** |
| **Línea Estratégica** | Comité de Gestión y Desempeño Institucional Y Comité Institucional de Control Interno | * Definir y aprobar el marco general para la gestión del riesgo y el control
* Analizar los riesgos, vulnerabilidades y amenazas institucionales para el cumplimiento de los objetivos estratégicos, planes institucionales, metas y compromisos de la entidad.
* Definir y aprobar la política para la administración del riesgo
* Garantizar el cumplimiento de los planes para la gestión de riesgos de la entidad
 |
| **Líneas de defensa** | **Responsable** | **Actividades y Responsabilidades frente al riesgo** |
| **Primera Línea** | Responsables y Líderes de Proceso, servidores públicos y colaboradores de la entidad | * Identificar, valorar, evaluar y actualizar como mínimo 1 vez al año o cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso.
* Establecer, aplicar y hacer seguimiento a la eficacia de los controles para mitigar los riesgos identificados, proponiendo e implementando las mejoras o acciones de tratamiento para su buena gestión.
* Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
* Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.
* Informar a la Secretaría General – coordinación del Sistema de Gestión, como segunda línea de defensa y a la oficina de control interno, sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo, para que se tomen las medidas pertinentes.
* Reportar a la coordinación del Sistema de Gestión los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos, para actualizar el Sistema de información que lo soporta.
 |
| **Segunda Línea** | Secretaría General - Coordinación del Sistema de Gestión | * Responder ante la línea estratégica sobre el estado en que se encuentran los riesgos, diseño de herramientas y acompañamiento en el proceso de aplicación
* 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 residual.
* Analizar, diseñar, adecuar, socializar y capacitar a las diferentes instancias sobre las metodologías y documentos internos establecidos en el Sistema de gestión, para la aplicación y gestión de los riesgos de gestión, corrupción y seguridad digital, conforme a las normativas y lineamientos vigentes.
* Consolidar el mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos), y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional.
* Presentar al Comité Institucional de Coordinación de Control Interno, cuándo éste lo requiera, la política de riesgos y el resultado de la medición del nivel de eficacia de los controles y el comportamiento de los riesgos identificados en los diferentes procesos de la entidad, conforme a las acciones de tratamiento establecidas, para que se tomen las acciones correspondientes
* Acompañar y orientar metodológicamente a los responsables y líderes de procesos, servidores públicos y colaboradores en la identificación, valoración, tratamiento y seguimiento de los riesgos de gestión, corrupción y seguridad digital, como mínimo 1 vez al año, en coordinación con Tic y el Dpto. Adtivo. De Planeación
* Supervisar que la primera línea identifique, analice, valore, evalué y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos.
 |
| **Tercera Línea** | Oficina de Control Interno | * Proporcionar un aseguramiento objetivo a la Alta Dirección sobre el diseño y efectividad de las actividades de administración del riesgo en la entidad con el fin de ayudar a asegurar que los riesgos claves o estratégicos estén adecuadamente definidos, sean gestionados apropiadamente y que el sistema de control interno está siendo operado efectivamente
* Comunicar al comité de coordinación de control interno los cambios e impactos en la evaluación del riesgo que resulten de la evaluación independiente
* Evaluar la efectividad de la Gestión del Riesgo en la Entidad, así como la adecuada aplicación de controles, planes de contingencia y actividades de monitoreo vinculados a riesgos clave en la entidad
* Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa
* Recomendar mejoras concretas a la política de operación para la administración del riesgo, y el adecuado diseño de controles establecidos
* Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.
* Evaluar que la gestión de los riesgos esté acorde con la política de la entidad y que sean monitoreados por la primera línea de defensa.
 |

# **METOLODOLOGIA GENERAL PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE CORRUPCIÓN, GESTIÓN Y SEGURIDAD DIGITAL.**

El establecimiento de la presente política de operación para la administración de los Riesgos de Gestión, corrupción, seguridad digital y diseño de controles en la Gobernación del Huila, partió del análisis de contexto estratégico y de la estructura de operación por procesos que tiene la entidad, esto es, la misión, visión, objetivos estratégicos, planeación institucional y los procesos actualmente vigentes.

**HERRAMIENTA DE TRABAJO EN EXCEL PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL**

El objetivo de la herramienta en Excel para identificar, valorar, tratamiento y seguimiento a los riesgos los riesgos de gestión, de corrupción y de seguridad digital, es estandarizar, minimizar la subjetividad y facilitar la trazabilidad y análisis del estado de los riesgos de la entidad, a fin de que se tomen las acciones correspondiente por parte de la línea estratégica y las 3 líneas de defensa correspondiente.

Esta herramienta y política de Administración de los Riesgos, hace parte del proceso de “Mejora continua” ubicado en la página de la Extranet / Sistema de Gestión MIPG / Operación de MIPG / Gestión del conocimiento. Igualmente esta herramienta conforme a la versión vigente, será objeto de mejora continua. Así mismo, será divulgada, socializada mediante procesos de capacitación y entrenamiento para que los responsables tengan uso y apropiación

Link:

http://extranet.huila.gov.co / sistema de Gestión MIPG / Operación MIPG / Gestión del conocimiento / Mejora continua

Esta herramienta fue rediseñada en Excel, con base en la Guía para la Administración del riesgo del DAFP, versión 4 de octubre de 2018 y los 4 anexos asociados, la cual contiene 11 hojas: la metodología general de administración de riesgos y 10 hojas adicionales con formatos estandarizados y controlados por el sistema de gestión, asociados a cada una de las fases de identificación, valoración, tratamiento y seguimiento, así:

A partir de la Hoja # 2, están los 10 formatos que contiene hojas de trabajo (sin color) o consulta (color azul), que están asociadas a las siguientes etapas o fases, así:

1. **Mapa y Plan de tratamiento de riesgos – SGN-C048-PR001-F14**: Hoja que resume el mapa por proceso para los 3 tipos de riesgos que se administran y solo permite la consulta e impresión, y se genera automáticamente a partir de la siguiente matriz.
2. **Matriz de identificación, valoración, tratamiento y seguimiento de riesgos de gestión, corrupción y seguridad digital – SGN-C048-PR001-F01**: Matriz que contiene la Hoja de trabajo que articula e integra los criterios y análisis para identificar, valorar, diseño adecuado de controles y tratamiento para cada uno de los riesgos, es decir, articula e integra los contenidos de los formatos establecidos en todas las hojas de esta herramienta en excel. Esta matriz permite el registro de la información relacionada con las fases de identificación, valoración y tratamiento de cada uno de los riesgos de Gestión, corrupción y seguridad digital establecidos en cada proceso. Esta matriz contiene varias columnas y celdas bloqueadas que contienen fórmulas de cálculo y validación. Igualmente esta matriz contiene las ayudas (comentarios) y conceptos básicos a fin de facilitar la aplicación y desarrollo de cada fase.
3. **Análisis del contexto para la administración de los riesgos de gestión, corrupción y seguridad digital- SGN-C048-PR001-F02:** Este formato contiene el análisis de contexto interno, externo y del proceso, que facilita la identificación de los posibles riesgos, las causas y las oportunidades, que deben ser tenidas en cuenta para el diligenciamiento de la matriz según formato SGN-C048-PR001-F01. Para mayor conocimiento de herramienta y análisis consultar el Anexo 2 Técnicas para el Establecimiento del Contexto y Valoración del Riesgo - Guía de riesgos 2018
4. **Criterios para identificar los activos y riesgos de seguridad digital- SGN-C048-PR001-F05.** Este formato solo aplica para los riesgos de seguridad digital. Para su buen diligenciamiento es fundamental consultar el ítems 4.1.6 del anexo 4: Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018.
5. **Criterios para definir e identificar los riesgos de corrupción- SGN-C048-PR001-F04:** Este formato para ser diligenciado y contiene criterios que deben cumplir los riesgos clasificados como corrupción. Si alguno de estos criterios no se cumplen, este riesgo no puede ser considerado riesgo de corrupción y podría considerarse como riesgo de gestión
6. **Criterios para identificar y redactar riesgos de gestión – SGN-C048-PR001-F06**: Este formato es solo de consulta, ya que contiene 4 preguntas básicas para identificar riesgos de gestión; también contiene algunas técnicas para redactar dichos riesgos de gestión y finalmente contiene 3 tablas como ejemplos de descripción de riesgos de gestión, corrupción y seguridad digital
7. **Criterios para valorar riesgos de gestión, corrupción y seguridad digital - SGN-C048-PR001-F07:** Este formato es solo de consulta, ya que contiene el mapa de calor que establece los 5 niveles de probabilidad y los 5 niveles de impacto. También contiene la tabla de las posibles combinaciones entre probabilidad e impacto, sobre las cuales se establecen las políticas de tratamiento, según corresponda la valoración preliminar y/o calificación final del riesgo. También contiene los conceptos de qué busca la fase de valoración de riesgos, haciendo énfasis en el análisis de los riesgos (riesgo inherente) y la evaluación de los riesgos (riesgo residual, es decir, después de aplicar controles). Igualmente contiene la Estrategia de Tratamiento en la Gobernación del Huila para hacer tratamiento y seguimiento, según la zona donde se ubique el riesgo y de acuerdo al tipo de riesgo (de gestión, corrupción o seguridad digital)
8. **Criterios de análisis (probabilidad e impacto), para valorar riesgos de gestión, corrupción y seguridad digital- SGN-C048-PR001-F08:** Este formato es solo de consulta, ya que contiene los criterios los criterios para determinar el nivel de probabilidad (que es igual para los 3 tipos de riesgos) y los 3 criterios distintos para determinar el nivel de impacto para los riesgos de gestión, corrupción y seguridad digital. También contiene Matriz de priorización de probabilidad según sea la participación activa del equipo de trabajo. La cual si debe ser diligenciada.
9. **Evaluación de controles para riesgos de gestión, corrupción y seguridad digital– SGN-C048-PR001-F03:** Formato que debe ser diligenciado y contiene los 6 criterios de evaluación en el diseño de controles, así como el peso de la evaluación de éstos 6 criterios, por cada causa de cada riesgo identificado. Así mismo, en este formato se debe diligenciar el responsable, la periodicidad de aplicación del control, propósito y cómo se realiza el control.
10. **Matriz de trazabilidad riesgos de gestión, corrupción y seguridad digital – SGN-C048-PR001-F013:**  Matriz que realiza el consolidado y permite la trazabilidad de todos los tipos de riesgos identificados desde la fecha inicial, y las diferentes valoraciones realizadas en cada año, mostrando el nivel del riesgo residual de cada valoración. También consolida los controles existentes y el estado en que se encuentra el riesgo. Esta matriz facilita la generación de análisis e informes.
11. **ETAPAS PARA LA GESTIÓN DE LOS RIESGOS**

Previo a realizar el análisis y levantamiento de la información para la administración de los riesgos asociados a los procesos de la entidad, es fundamental, que consulte y analice las Hojas # 1 (metodología general), 2 (mapa de riesgos) y 3 (1.matriz de identificación-2.valoración de Riesgos de Gestión, Corrupción y Seguridad Digital) de la herramienta en Excel diseñada, a fin de tener una visión clara y completa de todas las fases y resultados que se esperan de la administración de los 3 tipos de riesgos de la entidad, definidas conforme a la presente Política de Riesgos

* 1. **IDENTIFICACIÓN**

**Identificación Riesgos de Gestión:**

1. Realizar y/o consultar el análisis de contexto interno, externo y de proceso del formato “# 1.1 análisis de contexto” de la Hoja # 4 de la herramienta de excel para riesgos.
2. Consultar la hoja # 7 de “1.4.Técnicas identificar y redactar Riesgos”, considerando el concepto de Riesgo de Gestión y las preguntas asociadas para Identificar la afectación del cumplimiento del objetivo estratégico o del proceso, de tal forma que responsa a las preguntas: ¿QUÉ PUEDE SUCEDER?, ¿CÓMO PUEDE SUCEDER? ¿CUANDO PUEDE SUCEDER? ¿QUE CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?. Así mismo tener en cuenta las técnicas para la redacción de los riesgos de gestión, tal como se muestra el ejemplo de descripción de riesgo de gestión establecido en este formato.
3. Diligenciar las columnas “c” a la “n” de la hoja # 3 de “Matriz identificación-valoración Riesgos de Gestión Corrupción y Seguridad Digital”, con base en la información de los pasos 1 y 2. Conforme a la clasificación de riesgos de gestión. Teniendo en cuenta que la columna j, k y l aplica sólo para riesgos de seguridad digital.

**Identificación Riesgos de Corrupción:**

1. Realizar y/o consultar el análisis de contexto interno, externo y de proceso del formato “# 1.1 análisis de contexto” de la Hoja # 4 de la herramienta de excel para riesgos de corrupción.
2. Consultar y diligenciar la hoja # 6 de “1.3.identificación Riesgos de Corrupción”, considerando el concepto de Riesgo de Corrupción, diligenciar las 4 condiciones que debe cumplir para ser un riesgo de corrupción (ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO), conforme a la “Matriz definición del Riesgo de Corrupción”, teniendo presente el ejemplo de descripción de riesgo de corrupción establecido en este formato.
3. Diligenciar las columnas de la “A” a la “n” de la hoja # 3 de “Matriz identificación-valoración Riesgos de Gestión Corrupción y Seguridad Digital”, con base en la información de los pasos 1 y 2. Conforme a la clasificación de riesgos de corrupción. Teniendo en cuenta que la columna j, k y l aplican sólo para riesgos de seguridad digital.

**Identificación Riesgos de Seguridad digital:**

1. Realizar y/o consultar el análisis de contexto interno, externo y de proceso del formato “# 1.1 análisis de contexto” de la Hoja # 4 de la herramienta de excel para riesgos de Seguridad Digital.
2. Consultar y diligenciar la hoja # 5 de “1.3.identifificación Activos y Riesgos de Seguridad Digital”, considerando el concepto de Riesgo de Seguridad digital, diligenciando los 10 pasos para identificar los Activos de Seguridad digital asociados al proceso, teniendo presente el ejemplo de descripción de riesgo de seguridad digital establecido en este formato identificar los riesgos de seguridad digital que serán registrados en la “Matriz identificación-valoración Riesgos de Gestión Corrupción y Seguridad Digital”.
3. Diligenciar las columnas de la “A” a la “n” de la hoja # 3 de “Matriz identificación-valoración Riesgos de Gestión Corrupción y Seguridad Digital”, con base en la información de los pasos 1 y 2. Conforme a la clasificación de riesgos de seguridad digital.
	1. **VALORACIÓN**

**Análisis preliminar (Riesgo inherente) del Riesgo de Gestión, corrupción y seguridad digital.**

1. Diligenciar las columnas de la “O” a la “AB” de la “Matriz identificación-valoración Riesgos de Gestión, Corrupción y Seguridad Digital” relacionadas con el “Análisis preliminar del Riesgo – Riesgo inherente”, seleccionando la probabilidad e impacto (consecuencia), teniendo en cuenta los criterios de las tablas establecidos en la hoja # 9 de “2.1.Análisis (probabilidad-Impacto)”, así: “Tabla para determinar probabilidad en los Riesgos de Gestión, corrupción y seguridad digital”, considerando que es común para los 3 tipos de riesgos. Y la “Tabla para determinar impacto”, teniendo presente que se aplican tablas diferentes para cada uno de los 3 tipos de riesgos, así: “CRITERIOS PARA ESTABLECER EL NIVEL DE IMPACTO DE LOS RIESGOS DE GESTIÓN”, “CRITERIOS PARA ESTABLECER EL NIVEL DE IMPACTO DE LOS RIESGOS DE CORRUPCIÓN” y “CRITERIOS PARA ESTABLECER EL NIVEL DE IMPACTO DE LOS RIESGOS DE SEGURIDAD DIGITAL” que se presentan. **PERO TENIENDO EN CUENTA QUE EL NIVEL DE PROBABILIDAD (rara vez e improbable) y el NIVEL DE IMPACTO (insignificante y menor), NO APLICAN PARA LOS RIESGOS DE CORRUPCIÓN**
2. Una vez seleccionada la probabilidad e impacto del paso anterior, automáticamente aparecerá el “nivel de riesgo inherente”, el cual se calcula conforme a los criterios establecidos en la hoja # 8 “2.Criterios valoración de Riesgos” que contiene las posibles combinaciones de probabilidad e impacto, generando el nivel de exposición (bajo, moderado, alto y extremo); la valoración del riesgo (entre aceptables, tolerables, moderados, altos e inaceptables) y la zona: baja, moderada, alta y extrema

**Diseño y ejecución de controles (aplica para los riesgos de Gestión, Corrupción y Seguridad Digital)**

Para esta fase la herramienta en excel a través de las columnas de la “AC” a “AJ” realiza la “VALORACIÓN DE CONTROLES EXISTENTES”, ligando la hoja # 10 de “3. Evaluación de controles”, así:

1. En la columna “AC” se debe Seleccionar si el riesgo tiene asociado un control y de ser afirmativo, debe diligenciar la hoja # 10 de “3.Evaluación controles R.GCSD”, que le permitirá realizar la evaluación del controles asociados a cada una de las causas establecidas de los riesgos identificados, la cual contiene los 6 criterios de evaluación en el diseño adecuado de controles, así mismo, en este formato se debe diligenciar el responsable, la periodicidad de aplicación del control, propósito y cómo se realiza el control. Automáticamente la herramienta calcula el “Peso en la evaluación del diseño del control” de éstos 6 criterios, que se calcula con base en los criterios de (Fuerte (96-100) - Moderado (86-95) - Débil (0-85), llevándolo automáticamente a la columna “AD” de la “Matriz identificación-valoración Riesgos de Gestión, Corrupción y Seguridad Digital”, **considerando que si el resultado de ésta evaluación de diseño de control está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados**
2. Diligenciar la columna “AE” de “Calificación de la ejecución del control”, seleccionando de acuerdo con los criterios de: (Fuerte: Siempre se ejecuta) o (Moderado: Algunas veces se ejecuta) o (Débil: No se ejecuta)
3. La columna “AF” calcula automáticamente la “Solidez individual del control, con base en los criterios: ( Fuerte = 100), (Moderado=50), (Débil=0), teniendo presente 3 condiciones así: 1. SI fuerte (columna AO) + fuerte (siempre se ejecuta) = FUERTE (100); 2.fuerte (columna AO) + Moderado (algunas veces se ejecuta) = Moderado (50) y Ver todas las posibles combinaciones columna AO y AP (ver hoja1. Escondida y protegida por fórmulas)
4. La columna “AG” de “Peso en la evaluación del diseño del control” se calcula automáticamente con base en la condición: SI=100 y NO=0
5. La columna “AH” de “CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES”, se calcula automáticamente, con el promedio aritmético simple de los controles por cada riesgo, así: (FUERTE: Promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100), (MODERADO: El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99) y (DÉBIL: El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor de 50)
6. Diligenciar las columnas “AI” y “AJ”, seleccionando las opciones establecidas que determinan si los Controles ayudan a disminuir la probabilidad y el impacto?

**Evaluación del Riesgo VS Controles (Riesgo residual)**

1. Las columnas de la “AK” a la “AX” de la “Matriz identificación-valoración Riesgos de Gestión, Corrupción y Seguridad Digital” relacionadas con el “**Evaluación del Riesgo VS Controles (Riesgo residual**”, se calculan automáticamente considerando la tabla 8 de la guía # 3.2.3 de “resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos, teniendo en cuenta los resultados de la evaluación de controles. Considerando que “si la solidez del conjunto de controles es débil, éste no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo” y que “tratándose de riesgos de corrupción, únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento, teniendo en cuenta que **EL NIVEL DE PROBABILIDAD (rara vez e improbable) y el NIVEL DE IMPACTO (insignificante y menor), NO APLICAN PARA LOS RIESGOS DE CORRUPCIÓN –**
2. .Generando automáticamente el “NIVEL DEL RIESGO RESIDUAL” calificado como: bajo o moderado o alto o extremo.
	1. **TRATAMIENTO Y SEGUIMIENTO**

Las columnas de la “AY” a la “BB” de la “Matriz identificación-valoración Riesgos de Gestión, Corrupción y Seguridad Digital” Trae automáticamente las “**POLÍTICAS Y OPCIONES DE TRATAMIENTO DEL RIESGO**”, considerando la “TABLA DE POLITICA DE TRATAMIENTO Y SEGUIMIENTO, SEGÚN EL TIPO DE RIESGO Y LA ZONA DONDE SE UBIQUE EL RIESGO RESIDUAL”, que se encuentra en la hoja # 8 de “2.Criterios valoración de Riesgos”, que trae los NIVELES DE ACEPTACIÓN, así:

|  |  |  |
| --- | --- | --- |
| **Tipo de Riesgo** | **Zona del Riesgo** | **Estrategia de Tratamiento en la Gobernación del Huila** |
| Riesgos de Gestión y Seguridad digital | Baja | Se ACEPTA el riesgo y se administra por medio de las actividades propias del proceso o proyecto asociado y se realiza en el reporte **mensual** de su desempeño. |
| Moderada | Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad o el impacto de ocurrencia del riesgo, se hace seguimiento BIMESTRAL y se realizan acciones para su tratamiento, registran sus avances en la matriz de seguimiento de Riesgos - SGI |
| Alta y Extrema | Se debe incluir el riesgo tanto en el mapa de riesgo del proceso como en la matriz consolidada de riesgo y se establecen acciones de control preventivas que permitan EVITAR la materialización del riesgo. Se monitorea MENSUALMENTE y se registra en la matriz de seguimiento de Riesgos - SGI |
| Riesgos de Corrupción | Baja | NINGÚN riesgo de corrupción podrá ser ACEPTADO. Periodicidad de seguimiento MENSUAL para evitar a toda costa su materialización por parte de los procesos a cargo de estos riesgos |
| Moderada | Se establecer acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. Periodicidad de seguimiento MENSUAL para evitar a toda costa su materialización por parte de los procesos a cargo de estos y se registra en la matriz de seguimiento de Riesgos - SGI |
| Alta y Extrema | Se adoptan medidas para: REDUCIR la probabilidad, el impacto o ambos factores del riesgo; la estrategia conlleva a la implementación de controles.EVITAR Se abandonan o modifican las actividades que dan lugar al riesgo, decidiendo no iniciar, no continuar o modificar de forma segura la actividad que causa el riesgo.COMPARTIR con un tercero el tratamiento de una parte del riesgo para reducir la probabilidad, el impacto o ambos factores.Periodicidad de seguimiento MENSUAL para evitar a toda costa su materialización por partede los procesos a cargo de los mismos y se registra la matriz de seguimiento de Riesgos - SGI |

**Niveles de Aceptación**

Todos los riesgos de gestión y seguridad digital que se encuentran en una zona de riesgo alta y extrema, se realizará seguimiento mensual y se realizarán las acciones de tratamiento correspondiente. Los riesgos que se ubican en la zona de riesgo moderado, se realiza seguimiento bimensual y se realizan acciones para su tratamiento

Todos los riesgos de corrupción que se encuentren en cualquier zona de riesgo, se les realizará seguimiento mensual, a fin de evitar su materialización.

**MECANISMOS DE SEGUIMIENTO Y CONTROL A LOS RIESGOS**

Auditorías internas y externas de control independiente

Auditorías internas y externas de calidad

Seguimiento a las acciones de tratamiento y/o planes por parte de la Coordinación del Sistema de Gestión

Seguimiento a riesgos, diseño y aplicación de controles de la oficina de control interno

Capacitaciones a las instancias y líderes de proceso, por parte de Coordinación del Sistema de Gestión y de la oficina de control interno

Informe del Estado de los Riesgos a las instancias de Comités de Gestión desempeño institucional y/o departamental, como mínimo 1 vez al año por parte de la Coordinación del Sistema de Gestión y publicación en la extranet – Sistema de gestión

Publicación anual de los mapas de riesgos de gestión, corrupción y seguridad digital, en página web – link de transparencia, por parte de la coordinación del Sistema de gestión

# **TERMINOS Y DEFINICIONES**

* **CICCI:** Comité Institucional de Coordinación de Control Interno
* **CGDI:** Comité de Gestión y Desempeño Institucional
* **SGI:** Sistema de Gestión Integrado
* **MECI:** Modelo Estándar de Control Interno
* **MIPG:** Modelo Integrado de Planeación y Gestión
* **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 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 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 aspecto relacionados con el ambiente físico, digital y las personas.
* **Riesgo inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
* **Riesgo Residual:** Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
* **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
* **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.
* **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
* **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
* **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.
* **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.
* **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.
* **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.
* **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
* **Control:** Medida que modifica el riesgo bien modificando la probabilidad de ocurrencia o el impacto del evento de riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
* **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
* **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
* **Integridad**: propiedad de exactitud y completitud.
* **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
* **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.
* **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener o aceptar.

El apetito de riesgo y la tolerancia al riesgo son dos términos ampliamente usados, pero pueden ser fácilmente mal entendidos. Es por esta razón que a continuación compartimos algunos comentarios respecto a estos elementos que debemos tener en cuenta los auditores internos:

El apetito es el nivel de riesgo que la empresa quiere aceptar y su tolerancia es la desviación respecto a este nivel. La capacidad es el máximo de riesgo que una organización puede soportar en la persecución de sus objetivos.



**SOPORTE NORMATIVO Y DE REFERENCIA**

* Noma Técnica Colombiana NTC ISO 31000:2011. Gestión del Riesgo. Términos y Definiciones.
* Noma Técnica Colombiana NTC ISO 31000:2011 Sobre Gestión riesgo.
* Decreto 1499 del 11 de septiembre de 2017 “por medio del cual se modifica el Decreto 1083 de 2015, Decreto único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015”.
* Manual Operativo Sistema de Gestión del Modelo Integrado de Planeación y Gestión – MIPG, de fecha agosto de 2018
* Artículo 2.2.23.2 del Decreto 1499 de 2017, “Actualización del Modelo Estandar de Control Interno, que “se efectuará a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG”, Dimensión 7 - Sistema de control interno
* “Guía para la Administración del riesgo y el diseño de controles en entidades públicas”, Riesgos de Gestión, corrupción y seguridad digital, versión 4 de Función Pública, octubre de 2018
* LEY 1474 DE 2011, art. 73 Estatuto Anticorrupción.
* DECRETO 2641 DE 2012. Reglamenta los artículos 73 y 76 del Estatuto Anticorrupción.
* DECRETO 1081 DE 2015. Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República (compila disposiciones).
* Decreto 1083 de 2015, Cap. 5. “ELEMENTOS TÉCNICOS Y ADMINISTRATIVOS QUE FORTALEZCAN EL SISTEMA DE CONTROL INTERNO DE LAS ENTIDADES Y ORGANISMOS DEL ESTADO. Art. 2.2.21.5.1 Racionalización de la gestión institucional - (Decreto 1537 de 2001, art. 1); Art. 2.2.21.5.2 Manuales de procedimientos. (Decreto 1537 de 2001, art. 2); ARTÍCULO 2.2.21.5.4 Administración de riesgos . (Decreto 1537 de 2001, art. 4)
* 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.
* Norma Técnica Colombiana NTC ISO 9001:15

# **ANEXOS - METODOLOGICOS**

* Guía para la administración del riesgos y el diseño de controles en las entidades públicas – riegos de gestión, corrupción y seguridad digital, Ver 4 - Oct 2018
* Anexo 1: Técnicas para el Establecimiento del Contexto y Valoración del Riesgo - Guía de riesgos
* Anexo 2: Identificación de Riesgos de Corrupción asociados a la Prestación de Trámites y Servicios
* Anexo 3: Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas
* Anexo 4: Análisis y priorización de causas
* Anexo 5: Matriz de seguimiento riesgos de corrupción

**REGISTRO QUE GENERA EL PROCESO**

1. Metodología general de riesgos de gestión, corrupción y seguridad digital.
2. Mapa y Plan de tratamiento de riesgos – SGN-C048-PR001-F14
3. Matriz de identificación, valoración, tratamiento y seguimiento de riesgos de gestión, corrupción y seguridad digital – SGN-C048-PR001-F01
4. Análisis Del Contexto Para La Administración De Los Riesgos De Gestión, Corrupción Y Seguridad Digital- SGN-C048-PR001-F02
5. Criterios Para Identificar Los Activos y riesgos De Seguridad Digital- SGN-C048-PR001-F05
6. Criterios Para Definir Los Riesgos De Corrupción- SGN-C048-PR001-F04
7. Criterios para identificar y redactar riesgos de gestión, corrupción y seguridad digital – SGN-C048-PR001-F06
8. Criterios para valorar riesgos de gestión, corrupción y seguridad digital - SGN-C048-PR001-F07
9. Criterios de análisis (probabilidad e impacto), para valorar riesgos de gestión, corrupción y seguridad digital- SGN-C048-PR001-F08
10. Evaluación de controles para riesgos de gestión y corrupción – SGN-C048-PR001-F03
11. Matriz de trazabilidad riesgos de gestión, corrupción y seguridad digital – SGN-C048-PR001-F013

# **CONTROL DE CAMBIOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Vigencia** | **Identificación de los cambios** | **Responsable** |
| 1 | 5 de Septiembre de 2007 | Primera versión | Gerente del Sistema de Gestión Integrado |
| 2 | 10 de Octubre de 2008 | Se ajustó toda la metodología para la identificación, análisis valoración y tratamiento de la gestión de los riesgos. | Gerente del Sistema de Gestión Integrado |
| 3 | 14 de Mayo de 2009 | Se modificó la codificación del procedimiento y de los formatos que se utilizan, y también se modifico el formato de Plan de Tratamiento o mejoramiento del riesgo. | Gerente del Sistema de Gestión Integrado |
| 4 | 04 de mayo de 2010 | Se modificó el formato del Plan de Tratamiento o Mejoramiento del Riesgo, y la descripción de la actividad No 12. | Gerente del Sistema de Gestión Integrado |
| 5 | 6 Noviembre de 2012 | Se ajustaron las actividades del proceso y se acondicionaron al procedimiento Elaboración y gestión documentos versión 7. | Gerente del Sistema de Gestión Integrado |
| 6  | 19 Diciembre de 2012 | Se ajustaron y se adicionaron actividades al proceso.  | Gerente del Sistema de Gestión Integrado |
| 7  | 27 Diciembre de 2013 | Se revisó y ajustó todo el procedimiento: objetivo, alcance, soporte normativo, condiciones generales, actividades y Documentos y registros  | Gerente del Sistema de Gestión Integrado |
| 8 | 1 Abril de 2014 | Se cambió de tipo de documento procedimiento a instructivo.Se actualizaron los documentos y registros, descripción las actividades del instructivo.Se actualizó la metodología utilizada para la administración de los riesgos basada en la norma ISO 31000. | Gerente del Sistema de Gestión Integrado |
| 9 | 18 de Agosto de 2016 | Se modificó el objeto del instructivo.Se actualizo el soporte normativo.Se modificó el ítem “Metodología utilizada para la administración de los riesgos” actualizando el numeral 4 “Evaluación de controles”, el numeral 5 “Evaluación del Riesgos VS Control” y el numeral 6 “Política y opciones de tratamiento del riesgo”. Se modificó el ítem “Tratamiento de los riesgos no controlados” y el ítem “Reporte y divulgación del estado del riesgo”. | Gerente del Sistema de Gestión Integrado |
| 10 | 01 de Marzo del 2018 | Se eliminó el ítem Origen del riesgo.Se adicionó el ítem #7 “PLAN DE MEJORAMINETO OBLIGATIRIO PARA LOS RIESGOS NO CONTROLADOS”, porque se incluyó este plan en la matriz de identificación, análisis y tratamiento de riesgos y se eliminó como formato independiente.\*Se eliminó el ítem #7 “TRATAMIENTO DE LOS RIESGOS NO CONTROLADOS” ya que esto se incluyó en el ítem “PLAN DE MEJORAMIENTO OBLIGATORIO PARA LOS RIESGOS NO CONTROLADOS.\*Se actualizó el formato del Ítem Documentos y registros del instructivo. Y Primera versión de Matriz de Riesgos de Corrupción (Se independizó de los Riesgos Operativos del Proceso) | Gerente del Sistema de Gestión Integrado |
| 11 | 04 de septiembre de 2019 | Se unificaron los instructivos: gestión y administración de los riesgos de corrupción(SGN-C048-G001) y gestión y administración de los riesgos de los procesos(SGN-C048-I801), y como resultado se creó la GUIA PARA LA ADMINISTRACION DEL RIESGO Y EL DISEÑO DE CONTROLES DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, conforme a la guía establecida por el DAFP versión 4 de Octubre del 2018 | Gerente del Sistema de Gestión Integrado |

**CARLOS JULIO GONZALEZ VILLA**

 Gobernador del Departamento del Huila

Presidente del Comité Institucional de Gestión y Desempeño

Integrantes del Comité Institucional de Gestión y Desempeño,

**RICARLO MONCALEANO PERDOMO FRANCISCO JAVIER RUIZ ORTIZ**

Director Departamento Administrativo Jurídico Secretario General del Departamento

**CARLOS EDUCARDO TRUJILLO G. LILIANA MERCEDES VASQUEZ S.**

Secretario de Hacienda Secretaria de Gobierno y Desarrollo C.

**RODNEY PERDOMO HURTADO**

Director del Dpto. Adtivo. De Planeación

Secretario Técnico del Comité Institucional de Gestión y Desempeño

Revisada por: La mesa de Trabajo conformada por las áreas de Planeación, atención al ciudadano, Tic, Control Disciplinario, calidad, Talento humano y jurídica

Proyectada por: MYRIAM EMIL VARGAS CABRERA, Coordinadora del Sistema de Gestión: Modelo Integrado de Planeación y Gestión