POLÍTICA DE ADMINISTRACIÓN DEL RIESGO Y OPORTUNIDADES

ADRIANA ESCOBAR GÓMEZ
CONTRALORA

ANSELMO PERDOMO LEIVA
JEFE OFICINA ASESORA DE PLANEACIÓN

SERGIO RAMIREZ RODRIGUEZ
JEFE CONTROL INTERNO

LUIS CARLOS DÍAZ CASTILLO
PROFESIONAL UNIVERSITATIO

NEIVA, AGOSTO DE 2019

INTRODUCCIÓN

La Contraloría Departamental del Huila en cumplimiento de los principios legales establecidos en el artículo segundo literales a) y f) de la Ley 87 de 1993 y demás normas que la han modificado y adicionado, establece el siguiente marco de referencia para la gestión de los riesgos y oportunidades a los que se ve expuesta la entidad en desarrollo de su misión constitucional y el cumplimiento de sus objetivos estratégicos.

Esta herramienta de gestión de riesgos y oportunidades permite a la entidad detectar en forma oportuna todos aquellos hechos que pueden obstruir o mejorar el desarrollo normal de su actividad, mediante un proceso sistemático que le brinda a la alta dirección una seguridad razonable en el logro de sus objetivos misionales y estratégicos.

La Política para la administración del riesgo y oportunidades se encuentra articulado con el Sistema de Gestión de Calidad, con el Sistema de Control Interno y se establece como un instrumento con enfoque preventivo y proactivo que permitirá el manejo de los riesgos mediante la aplicación de controles y su control y seguimiento.

Adicional a esto, determina los roles y responsabilidades de los servidores públicos de la Contraloría Departamental del Huila en la identificación, análisis, evaluación, aplicación de controles, su seguimiento y evaluación.

MARCO NORMATIVO

- Ley 87 de 1993
- Guía para la Administración del Riesgo DAFP versión 4
- Norma Técnica Colombiana GTC 137 de 2014
- NTC ISO 31000 – 2009 Gestión del Riesgo
- Decreto 1499 de 2017

TÉRMINOS Y DEFINICIONES

ACTIVO: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

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

APETITO AL RIESGO: Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

CADENA DE VALORES: La interrelación de los procesos dirigidos a satisfacer las necesidades y requisitos de los usuarios.

CARACTERIZACIÓN DE LOS PROCESOS: Estructura que permite identificar los rasgos distintivos de los procesos. Establece su objetivo, la relación con los demás procesos, los insumos, los activos, su transformación a través de las actividades que desarrolla y las salidas del proceso, se identifican los proveedores y clientes o usuarios, que pueden ser internos o externos.

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

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 (procesos, políticas, dispositivos, prácticas u otras acciones).

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

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.

INTEGRIDAD: Propiedad de exactitud y completitud.

MAPA DE RIESGOS: Documento con la información resultante de la gestión del riesgo.

MAPA O RED DE PROCESOS: Es la representación gráfica de los procesos estratégicos, misionales, de apoyo, de evaluación y sus interacciones. Constituye la razón de ser de la entidad, sintetiza los principales propósitos estratégicos y los va- lores esenciales que deben ser conocidos, comprendidos y compartidos por todas las personas que hacen parte de la entidad.

MODELO DE OPERACIÓN POR PROCESOS: El modelo de operación por procesos es el estándar organizacional que soporta la operación de la entidad pública, integrando las competencias constitucionales y legales que la rigen con el conjunto de planes y programas necesarios para el cumplimiento de su misión, visión y objetivos institucionales. Pretende determinar la mejor y más eficiente forma de ejecutar las operaciones de la entidad.

OBJETIVOS DEL PROCESO: Son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto, debe iniciarse con un verbo fuerte como: establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción.

OBJETIVOS ESTRATÉGICOS: Identifican la finalidad hacia la cual deben dirigirse los recursos y esfuerzos para dar cumplimiento al mandato legal aplicable a cada entidad. Estos objetivos institucionales se materializan a través de la ejecución de la planeación anual de cada entidad.

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.

PLANEACIÓN INSTITUCIONAL: Las estrategias de la entidad generalmente se definen por parte de la alta dirección y obedecen a la razón de ser que desarrolla la misma, a los planes sectoriales, las políticas específicas que define el Gobierno nacional, departamental o municipal enmarcadas dentro del Plan Nacional de Desarrollo. En este contexto la entidad define su planeación institucional.

La planeación institucional hace uso de los procesos estratégicos, misionales, de apoyo y evaluación para materializarla o ejecutarla, por lo tanto la administración del riesgo no puede verse de forma aislada.

RIESGO DE CORRUPCIÓN: Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.

RIESGO ESTRATÉGICO: Se asocia con la forma en que se administra la Entidad, su manejo se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

RIESGO FINANCIERO: Relacionado con el manejo de recursos, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo de los bienes.

RIESGO DE CUMPLIMIENTO: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

RIESGO DE IMAGEN: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución

RIESGO DE TECNOLOGÍA (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.

RIESGO INHERENTE: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto

RIESGO OPERATIVO: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

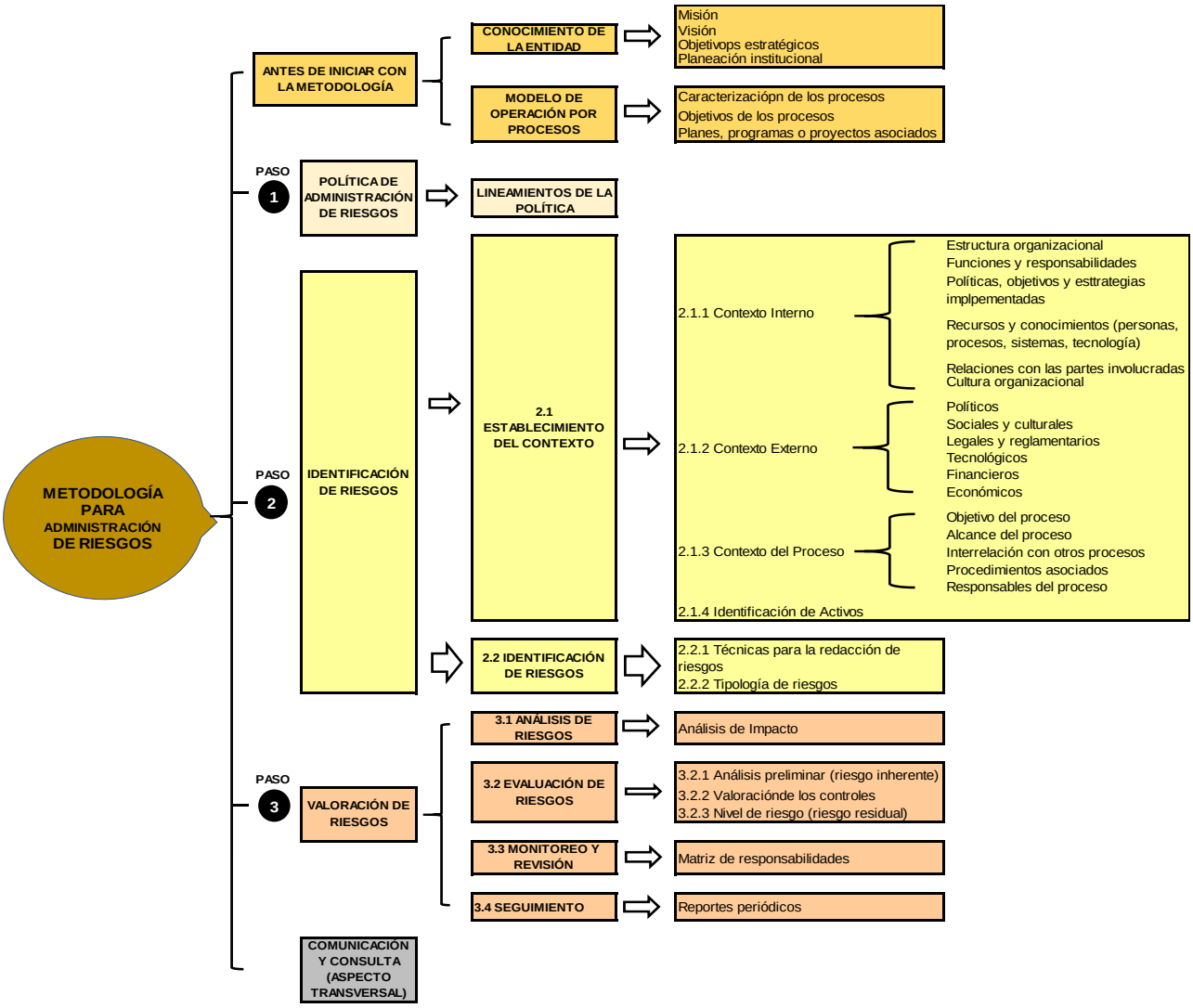
RIESGO RESIDUAL: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

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.

Es la proyección de la entidad a largo plazo que permite establecer su rumbo, las metas y lograr su desarrollo. Debe ser construida y desarrollada por la Alta Dirección de manera participativa, clara, amplia, positiva, coherente, convincente, comunicada y compartida por todos los miembros de la organización.

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

MARCO DE REFERENCIA PARA LA ADMINISTRACIÓN DEL RIESGO Y OPORTUNIDADES



POLÍTICA DE ADMINISTRACIÓN DEL RIESGO Y OPORTUNIDADES

La Contraloría Departamental del Huila como ente de control fiscal se compromete íntegramente a establecer en este documento las directrices generales para la gestión de los eventos que puedan afectar negativamente el desarrollo de la misión institucional, el cumplimiento de los objetivos estratégicos y su imagen ante la comunidad, mediante la adecuada comunicación, consulta, establecimiento del contexto, identificación, análisis, evaluación, tratamiento,

monitoreo y revisión de los riesgos y oportunidades, implementando las acciones de control que permitan su modificación.

La entidad establece las responsabilidades de los servidores públicos según el rol que cumplen de conformidad a sus funciones; así como las herramientas necesarias con la participación de los servidores públicos y contratistas para promover la integridad que permita controlar y responder a los acontecimientos potenciales o aquellos en los que puedan desencadenar situaciones de corrupción.

OBJETIVO

Establecer los controles que permitan asumir, reducir o mitigar eventos potenciales o materiales que impidan el desarrollo de la misión institucional, el cumplimiento de los objetivos estratégicos y su imagen ante la comunidad.

ALCANCE

Es aplicable a todo el sistema de gestión de la Contraloría Departamental del Huila, el cual se encuentra estructurado por procesos, y a las actuaciones de sus servidores públicos en cumplimiento de sus funciones constitucionales, legales e institucionales.

COMPROMISO DE LA ALTA DIRECCIÓN

La alta dirección de la Contraloría Departamental del Huila tiene un compromiso continuo en la implementación de la gestión del riesgo y oportunidades en la entidad, para lo cual le corresponde:

- Definir y aprobar la política para la gestión del riesgo y las oportunidades
- Definir y realizar seguimiento a los niveles de aceptación (apetito al riesgo)
- Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar alteraciones en la estructura de riesgos, controles y oportunidades.
- Realizar seguimiento y análisis periódico a los riesgos institucionales
- Evaluar el estado del sistema de control interno y aprobar sus modificaciones, actualizaciones y acciones de fortalecimiento.
- Garantizar la asignación de recursos necesarios para la gestión del riesgo y oportunidades.
- Comunicar los beneficios de la gestión del riesgo y oportunidades a todas las partes involucradas.
- Garantizar que el marco de referencia para gestionar los riesgos y oportunidades sea adecuado.

COMPROMISO DE LOS LÍDERES DE PROCESO

- Identificar y valorar los riesgos y oportunidades que pueden afectar los planes y procesos a su cargo y actualizarlos cuando se requiera con énfasis en la prevención del daño antijurídico.
- Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados en su proceso y proponer mejoras a su 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
- Informar a la oficina de planeación sobre los riesgos materializados en los planes y/o procesos a su cargo
- Reportar a la Oficina de Planeación el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar

COMPROMISO DE LA OFICINA ASESORA DE PLANEACIÓN

- 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
- 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 Dirección
- Apoyar al responsable del Control Interno en la orientación y entrenamiento a los líderes de procesos en la identificación, análisis y valoración del riesgo y oportunidades
- Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos
- Supervisar que los líderes de proceso identifiquen, evalúen y gestionen los riesgos, controles y oportunidades para que se generen acciones
- Evaluar que los riesgos y oportunidades sean consistentes con la presente política de la entidad y que sean monitoreados por los líderes de proceso

COMPROMISO DEL RESPONSABLE DE CONTROL INTERNO

- Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo, control y oportunidades, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos
- Orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo, diseño de controles y oportunidades

- Llevar a cabo el seguimiento a los riesgos y oportunidades consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al SGC
- Recomendar mejoras a la política de administración del riesgo y oportunidades

LINEAMIENTOS BÁSICOS DE LA GESTIÓN DEL RIESGO Y OPORTUNIDADES

- Para la identificación, análisis, evaluación, tratamiento, monitoreo y revisión de los riesgos y oportunidades de los procesos, se debe tener en cuenta el contexto externo asociado al objetivo del proceso y el contexto interno asociado a las actividades del proceso, los planes de mejoramiento, los productos no conformes, encuestas de satisfacción, resultados de la gestión del proceso, aplicando los lineamientos establecidos en esta política.

- Los líderes de procesos identificarán los eventos de conformidad a los tipos de riesgos que pueden ser: estratégicos, operativos, financieros, de gestión, seguridad digital y de corrupción entre otros.

- Las actividades de control que se establezcan para el tratamiento de los riesgos deben evidenciar su eficacia en la gestión efectiva de los riesgos identificados, de tal manera que se puedan reducir las posibilidades de ocurrencia y los impactos que puedan llegar a generar.

- Los riesgos de corrupción se gestionan a través de estos postulados y siempre tendrán en zona alta o extrema, con impacto catastrófico y debe establecerse controles dirigidos a evitar su materialización o su reducción, teniendo en cuenta lo estipulado en la Ley 1474 de 2011 y el Documento Estrategias para la construcción del plan anticorrupción y de atención al ciudadano.

- Los riesgos de seguridad digital se gestionan teniendo en cuenta además de las premisas aquí mencionadas, los lineamientos de la Guía de gestión de riesgos de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y Comunicaciones - MinTic.

- El monitoreo de los riesgos y oportunidades se realiza de manera integral (institucionales y de corrupción) en forma semestral.

- En los casos de que un riesgo se materialice, el líder de proceso debe establecer un plan de contingencia (acción correctiva).

- Es responsabilidad de los líderes de procesos verificar el cumplimiento de los planes de tratamiento establecidos (controles) para los riesgos identificados teniendo en cuenta tiempo y cronogramas determinados.

- Los riesgos que se encuentren en nivel de aceptación BAJO, que soporten documentación de sus controles en sus procedimientos y evidencien implementación de sus controles existentes y no presenten materialización durante la vigencia, pueden ser considerados para su eliminación.

TRATAMIENTO Y MANEJO DE LOS RIESGOS Y OPORTUNIDADES

La Contraloría Departamental del Huila dará tratamiento a los riesgos y oportunidades detectados en cumplimiento de la función institucional, sus objetivos estratégicos y los de proceso de acuerdo con la calificación de los riesgos residuales (riesgos después de controles), estableciendo los niveles de aceptación para cada uno y los controles o su tratamiento.

Identificación del Riesgo:

La Contraloría Departamental identifica las fuentes de riesgo, las áreas de impacto, los eventos y sus causas y consecuencias potenciales, con el objeto de generar un listado de todos los riesgos basándose en los eventos que podrían crear, aumentar, prevenir, degradar, acelerar, o retrasar el logro de los objetivos. Es importante identificar todos los riesgos a los que se encuentra expuesta la entidad con el objeto de analizar su probabilidad e impacto.

La Contraloría Departamental aplicará el proceso aquí establecido para determinar cuáles de ellos son los de mayor importancia de conformidad a sus consecuencias si llegare a materializarse para desarrollar e implementar los respectivos controles o correcciones.

La Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas establece lo siguiente:

IDENTIFICACIÓN DE RIESGOS

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

Las preguntas claves para la identificación del riesgo permiten determinar:

¿QUÉ PUEDE SUCEDER? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto.
¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo con el desarrollo del proceso.
¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo.

Ejemplos de descripción del riesgo

Formato de descripción del riesgo de gestión

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	La combinación de factores como insuficiente capacitación del personal de contratos, cambios en la regulación contractual, inadecuadas políticas de operación y carencia de controles en el procedimiento de contratación pueden ocasionar inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad y, en consecuencia, afectar la continuidad de su operación.	Operativo	Carencia de controles en el procedimiento de contratación Insuficiente capacitación del personal de contratos Desconocimiento de los cambios en la regulación contractual Inadecuadas políticas de operación	1. Parálisis en los procesos 2. Incumplimiento en la entrega de bienes y servicios a los grupos de valor 3. Demandas y demás acciones jurídicas 4. Detrimento de la imagen de la entidad ante sus grupos de valor 5. Investigaciones disciplinarias

RIESGO DE CORRUPCIÓN

Definición de riesgo de corrupción:

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).

Es necesario que en la descripción del riesgo concurran los **componentes de su definición**, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN

Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Formato de descripción del riesgo de corrupción

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin celebrar un contrato.	Situaciones como: debilidades en la etapa de la planeación del contrato, la excesiva discrecionalidad, las presiones indebidas, la carencia de controles, la falta de conocimiento y/o experiencia, sumados a la falta de integridad pueden generar un riesgo de corrupción en la contratación, como por ejemplo "exigencias de condiciones en los procesos de selección que solo cumple un determinado proponente".	Corrupción	Debilidades en la etapa de planeación, que faciliten la inclusión en los estudios previos, y/o en los pliegos de condiciones de requisitos orientados a favorecer a un proponente. Presiones indebidas. Carencia de controles en el procedimiento de contratación. Falta de conocimiento y/o experiencia del personal que maneja la contratación. Excesiva discrecionalidad. Adendas que modifican las condiciones generales del proceso de contratación para favorecer a un proponente.	1. Pérdida de la imagen institucional. 2. Demandas contra el Estado. 3. Pérdida de confianza en lo público. 4. Investigaciones penales, disciplinarias y fiscales. 5. Detrimento patrimonial. 6. Obras inconclusas. 7. Mala calidad de las obras. 8. Enriquecimiento ilícito de contratistas y/o servidores públicos.

Formato de descripción del riesgo de seguridad digital

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: **"Integridad, confidencialidad o disponibilidad"**

Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Seleccionar las vulnerabilidades asociadas a la amenaza identificada

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

Valoración del Riesgo

En esta situación se distinguen dos momentos:

Análisis del Riesgo:

En este evento se busca determinar la probabilidad de ocurrencia del riesgo y sus posibles consecuencias (impacto) tanto positiva como negativa en el desarrollo de las actividades, cumplimiento de su misión u objetivos estratégicos, así como la imagen institucional frente a la comunidad, con el objeto de establecer la zona de riesgo inicial (Riesgo Inherente). Es una entrada para su evaluación y para las decisiones sobre si es necesario o no tratarlo y las estrategias y métodos más adecuados para su tratamiento.

Su análisis involucra la consideración de las causas y sus fuentes y los factores que afectan las consecuencias y la probabilidad y otros atributos del riesgo. Así mismo, debe considerarse los controles existentes, su eficacia y eficiencia.

La forma en la cual las consecuencias y la probabilidad se expresan y el modo en el cual se combinan para determinar el nivel de riesgo, debe reflejar el tipo de riesgo, la información disponible y el propósito para el cual se va a usar la salida de su valoración, debe ser consistente con los criterios del riesgo; así mismo, es importante tener en cuenta la interdependencia de ellos y sus orígenes.

Tabla ilustrativa 1 - Probabilidad

Bajo el criterio de Probabilidad, el riesgo se debe medir a partir de las siguientes especificaciones[5]:

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Tabla ilustrativa 2 - Impacto

Bajo el criterio de Impacto, el riesgo se debe medir a partir de las siguientes especificaciones, contenidas en la tabla de impactos o consecuencias definida en la política de riesgos institucional:

Niveles para calificar el Impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.

Niveles para calificar el Impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
Menor	- Impacto que afecte la ejecución presupuestal en un valor ≤1% - Pérdida de cobertura en la prestación de los servicios de la entidad ≤5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≤1% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤1%del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
Insignificante	- Impacto que afecte la ejecución presupuestal en un valor ≤0,5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≤1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≤0,5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤0,5%del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Tabla 4. Criterios para calificar el impacto – riesgos de seguridad digital

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Para estimar el nivel de riesgo inicial los valores determinados para la probabilidad y el impacto o consecuencias se cruzan en la siguiente matriz de riesgo, con el fin de determinar la zona de riesgo en la cual se ubica el riesgo identificado. Este primer análisis del riesgo se denomina Riesgo Inherente[b] y se define como aquél al que se enfrenta una entidad en ausencia de acciones por parte de la Dirección para modificar su probabilidad o impacto

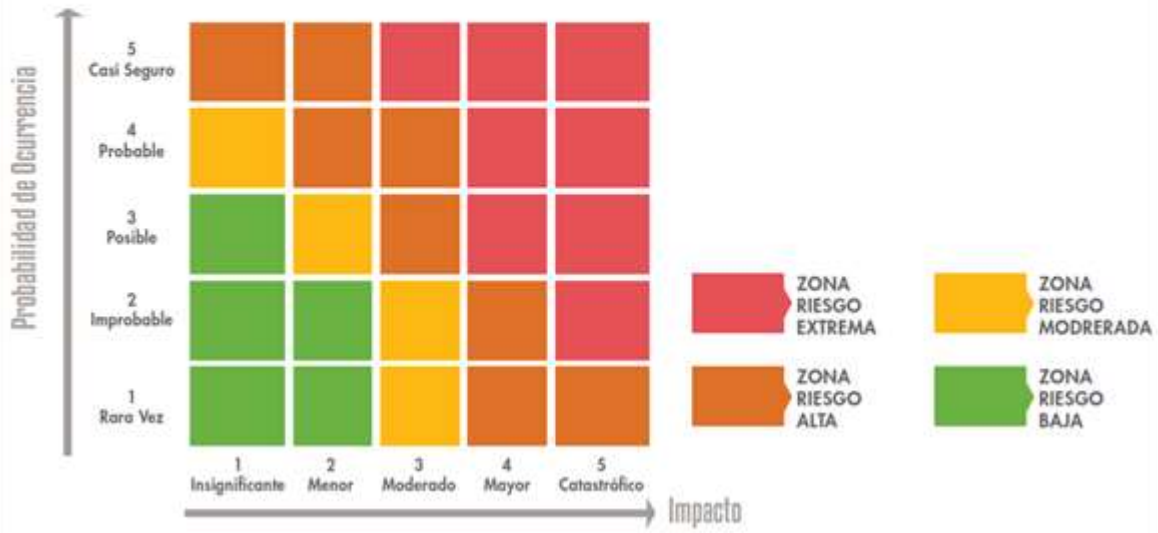


Tabla 5. Criterios para calificar el impacto - riesgos de corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		**10**	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

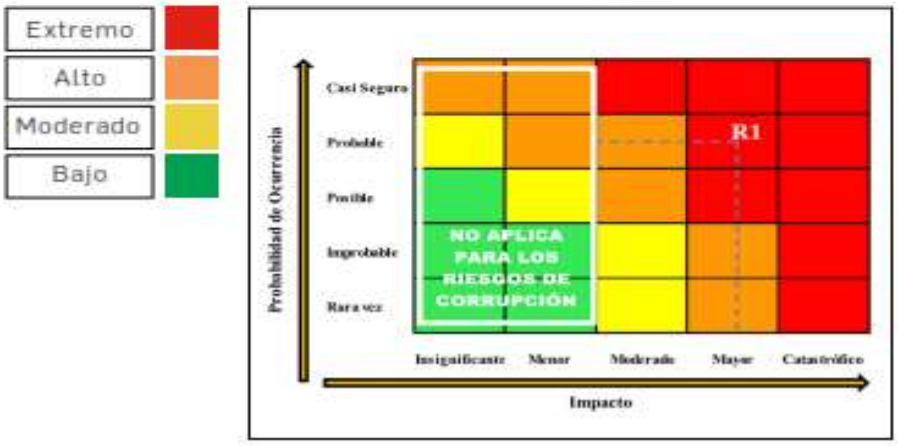
Nivel de impacto MAYOR

Análisis del impacto en riesgos de corrupción

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

De acuerdo con la tabla de criterios para calificar el impacto de la página anterior, nuestro ejemplo tiene un nivel de impacto MAYOR. La probabilidad de los riesgos de corrupción se califica con los mismos cinco niveles de los demás riesgos.

Por último ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente, para el ejemplo corresponde a: EXTREMO. R1



Evaluación o Valoración del Riesgo: El objetivo es confrontar los resultados del análisis del riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).

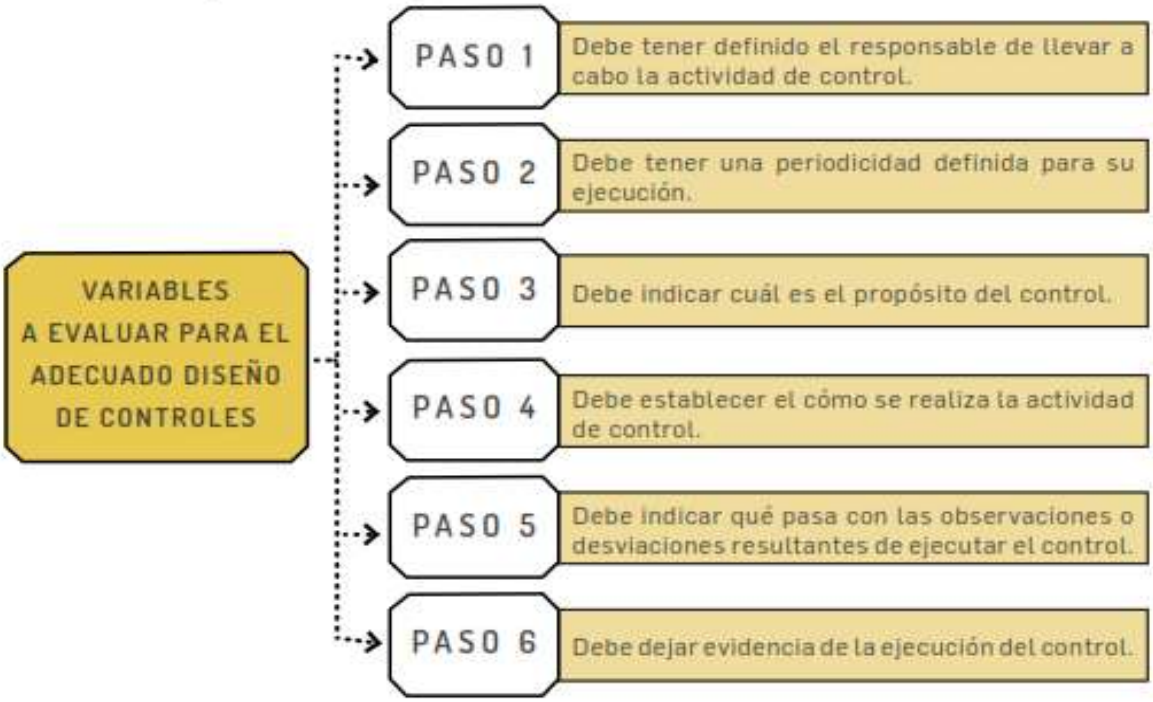
Valoración de los controles – diseño de controles

Antes de valorar los controles es necesario conocer cómo se diseña un control, para lo cual daremos respuesta a las siguientes interrogantes:

¿Cómo defino o establezco un control para que en su diseño mitigue de manera adecuada el riesgo?

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

Esquema 10. Pasos para diseñar un control



La Guía Técnica Colombiana 137 para la Administración del Riesgo establece los siguiente:

Valoración del Riesgo

Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

Acciones fundamentales para valorar el riesgo

- IDENTIFICAR CONTROLES EXISTENTES
- QUIÉN LLEVA A CABO EL CONTROL (RESPONSABLE)
- QUÉ BUSCA HACER EL CONTROL (OBJETIVO)
- CÓMO SE LLEVA A CABO EL CONTROL (PROCEDIMIENTO)
- EVIDENCIA DE LA EJECUCIÓN DEL CONTROL
- TIPO DE CONTROL (MANUAL O AUTOMÁTICO)
- CUÁNDO SE REALIZA EL CONTROL (PERIODICIDAD)

Posibles controles	
POLÍTICAS CLARAS APLICADAS	Políticas claras aplicadas
	Seguimiento al plan estratégico y operativo
	Indicadores de gestión
	Tableros de control
	Seguimiento a cronograma
	Informes de gestión
CONCILIACIONES	Conciliaciones
	Consecutivos
	Verificación de firmas
	Listas de chequeo
	Registro controlado
	Segregación de funciones
	Niveles de autorización
	Custodia apropiada
	Procedimientos formales aplicados
	Pólizas
	Seguridad física
	Contingencias y respaldo
	Personal capacitado
	Aseguramiento y calidad
NORMAS CLARAS Y APLICADAS	Normas claras y aplicadas
	Control de términos

Análisis y Evaluación de los Controles

La valoración del riesgo requiere de una evaluación de los controles existentes, lo cual implica:

a. Determinar su naturaleza:

Si se trata de un control preventivo, detectivo o correctivo, para este análisis tenga en cuenta:

CONTROLES PREVENTIVOS:
Evitan que un evento suceda. Por ejemplo el requerimiento de un login y password en un sistema de información es un control preventivo. Éste previene (teóricamente) que personas no autorizadas puedan ingresar al sistema. Dentro de esta categoría pueden existir controles de tipo detectivo, los cuales permiten registrar un evento después de que ha sucedido, por ejemplo, registro de las entradas de todas las actividades llevadas a cabo en el sistema de información, traza de los registros realizados, de las personas que ingresaron, entre otros.

CONTROLES CORRECTIVOS:
Éstos no prevén que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado. Por ejemplo en caso de un desastre natural u otra emergencia mediante las pólizas de seguro y otros mecanismos de recuperación de negocio o respaldo, es posible volver a recuperar las operaciones.

b. Determinar si los controles están documentados

de forma tal que es posible conocer cómo se lleva a cabo el control, quién es el responsable de su ejecución y cuál es la periodicidad para su ejecución, lo cual determinará las evidencias que van a respaldar la ejecución del mismo.

c. Establecer si el control que se implementa es automático o manual

CONTROLES AUTOMÁTICOS:
Utilizan herramientas tecnológicas como sistemas de información o software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros. Este tipo de controles suelen ser más efectivos en algunos ámbitos dada su complejidad.

CONTROLES MANUALES:
Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros.

d. Determinar si los controles se están aplicando en la actualidad

y si han sido efectivos para minimizar el riesgo.

Para realizar dicho análisis, a continuación se muestra una tabla ilustrativa, con el fin de orientar el análisis objetivo de los controles y de este modo poder determinar el desplazamiento dentro de la Matriz de Evaluación de Riesgos[3], las calificaciones planteadas para cada aspecto deben ser usadas tal como están expresadas, aplicar el valor asignado a cada aspecto si responde SI; cero (0) si responde NO. Es importante que no se asignen valores intermedios para evitar subjetividad en el análisis.

Tabla Ilustrativa 3 - Análisis y Evaluación de los controles

Descripción del control	Criterios para la evaluación	Evaluación		Observaciones
		Sí	No	
Describa el control determinado para el riesgo identificado	¿El control previene la materialización del riesgo (afecta probabilidad) ¿El control permite enfrentar la situación en caso de materialización (afecta impacto)?	N/A	N/A	Este criterio no puntúa, es relevante determinar si el control es preventivo (probabilidad) o si es correctivo que permite enfrentar el evento una vez materializado (impacto), con el fin de establecer el desplazamiento en la matriz de evaluación de riesgos.
	¿Existen manuales, instructivos o procedimientos para el manejo del control?	15	0	
	¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5	0	
	¿El control es automático? (Sistemas o Software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros).	15	0	
Descripción del control	**Criterios para la evaluación**	**Evaluación**		**Observaciones**
		Sí	**No**	
Describa el control determinado para el riesgo identificado	¿El control es manual? (Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros)	10	0	
	¿La frecuencia de ejecución del control y seguimiento es adecuada?	15	0	
	¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10	0	
	¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30	0	
	TOTAL	100	0	

Rangos de calificación de los controles	Dependiendo si el control afecta probabilidad o impacto desplaza en la matriz de evaluación del riesgo así: EN PROBABILIDAD AVANZA HACIA ABAJO EN IMPACTO AVANZA HACIA LA IZQUIERDA
	Cuadrantes a disminuir
Entre 0-50	0
Entre 51-75	1
Entre 76-100	2

Tabla 6. Análisis y evaluación de los controles para la mitigación de los riesgos.

Análisis y evaluación del diseño del control de acuerdo con las seis (6) variables establecidas:

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir o detectar	No es un control
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	No confiable
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	No se investigan y resuelven oportunamente.
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	Incompleta / no existe

Tabla 7. Peso o participación de cada variable en el diseño del control para la mitigación del riesgo

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

Resultado de la Evaluación de la Ejecución del Control

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO - PESO DE LA EJECUCIÓN DEL CONTROL -
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Análisis y evaluación de los Controles para la Mitigación de los Riesgos

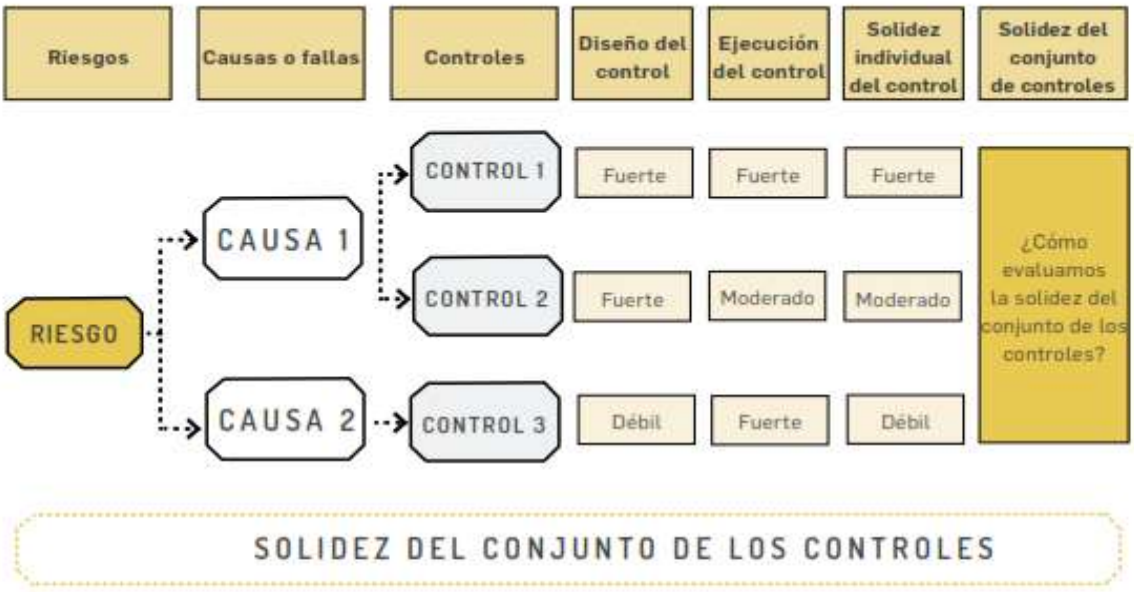
Se debe consolidar el conjunto de los controles asociados a las causas para evaluar si estos de manera individual y en conjunto ayudan al tratamiento de los riegos, considerando tanto el diseño, ejecución individual y el promedio de los controles.

En la evaluación del diseño y ejecución de los controles las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, de la siguiente forma.

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE:100 MODERADO:50 DÉBIL:0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ / NO
fuerte: calificación entre 96 y 100*	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Cuando existe más de un control para el riesgo, se debe evaluar la solidez de ellos:

Esquema 12. Solidez del conjunto de controles



SOLIDEZ DEL CONJUNTO DE LOS CONTROLES

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El 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.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

De igual forma como se establecen controles para mitigar su probabilidad, también se deben realizar con el objeto de disminuir su impacto en caso de materialización.

Nivel de Riesgo (Riesgo Residual)
Debido a que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

Tabla 8. Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos.

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES.	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
fuerte	directamente	directamente	2	2
fuerte	directamente	indirectamente	2	1
fuerte	directamente	no disminuye	2	0
fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	Indirectamente	1	0
moderado	directamente	no disminuye	1	0
moderado	no disminuye	directamente	0	1

IMPORTANTE

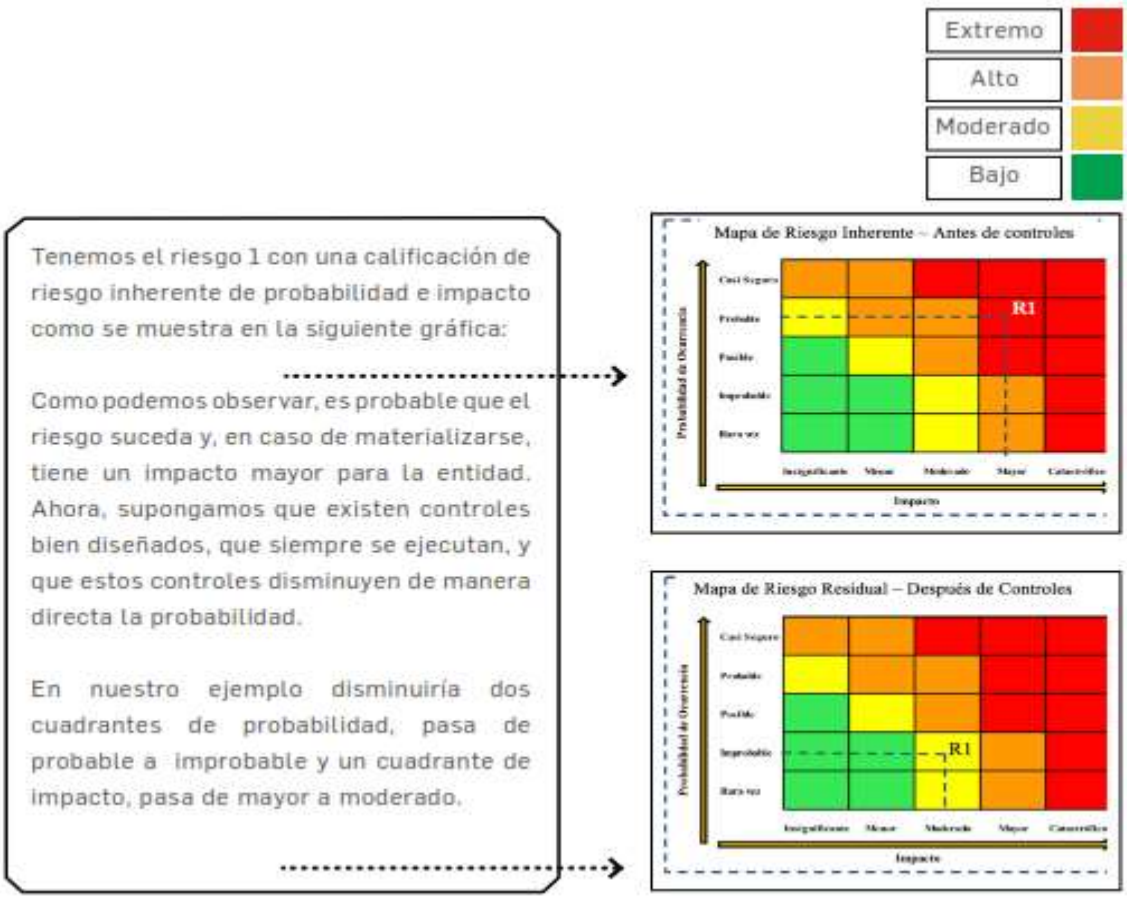
Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

IMPORTANTE

Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

Resultado del Mapa de Riesgo Residual:

Realizado el análisis y evaluación de los controles para la mitigación de los riesgos, se elabora el mapa de riesgo residual (después de los controles).



Tratamiento de los Riesgos

Es la respuesta que la Contraloría Departamental del Huila establece para mitigar el riesgo, incluyendo los relacionados con corrupción para los cuales la respuesta será evitarlos, compartirlos o reducirlos. En caso de que una respuesta se derive de un riesgo residual y supere los niveles de aceptación, se deberá volver a analizarlo y revisar sus controles.

La siguiente gráfica muestra las categorías de tratamiento de los riesgos que se tratan en la Contraloría Departamental del Huila:

Se acepta el riesgo cuando se encuentra dentro de la zona de calificación de riego bajo o cuando no se le puedan establecer controles, razón por la cual no es necesaria la implementación de controles que afecten la probabilidad o el impacto; sin embargo, debe existir un seguimiento continuo de ellos.

Se acepta el riesgo cuando sus escenarios no se encuentran al alcance de intervenirlos por medio de controles; es decir, cuando se encuentra por fuera de las atribuciones de la Contraloría Departamental del Huila.

Se evita el riesgo cuando son abandonadas las actividades que originan o que lo promueven y se decide no iniciar o continuar con aquellas acciones que son sus causantes o las que provocan que sucedan hechos de riesgo.

Se comparte el riesgo cuando se reduce la probabilidad o el impacto del riesgo y se transfiere o comparte con una o más dependencias de la entidad.

Se reduce el riesgo cuando la Contraloría Departamental del Huila adopta medidas para reducir su probabilidad o impacto u ambos a la vez, lo que conlleva a la implementación de controles apropiados y con una segregación de funciones si es del caso de tal forma que el tratamiento logre la reducción prevista.

Para tratar o mitigar los riesgos de seguridad digital se deben emplear los controles del anexo A de la ISO/IEC 27001/2013 que se encuentran en el anexo 4 de la "Guía para la administración del riesgo y el diseño de controles en las entidades públicas".

Las actividades de control o controles son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Las actividades de control se pueden clasificar de la siguiente forma:

Monitoreo y Revisión

La responsabilidad sobre el control de la gestión del riesgo y oportunidades en la Contraloría Departamental del Huila es desarrollada a través de las líneas de defensa en las cuales se encuentran los roles y responsabilidades de todos los actores del riesgo, proporcionando de esta forma aseguramiento de su gestión y previniendo su materialización en todos sus ámbitos.

El monitoreo y revisión de la gestión de los riesgos y oportunidades se encuentra bajo el esquema de control interno de la entidad, desarrollado mediante el

esquema MECI, a través de asignación de responsabilidades y roles, distribuido en de la siguiente forma:

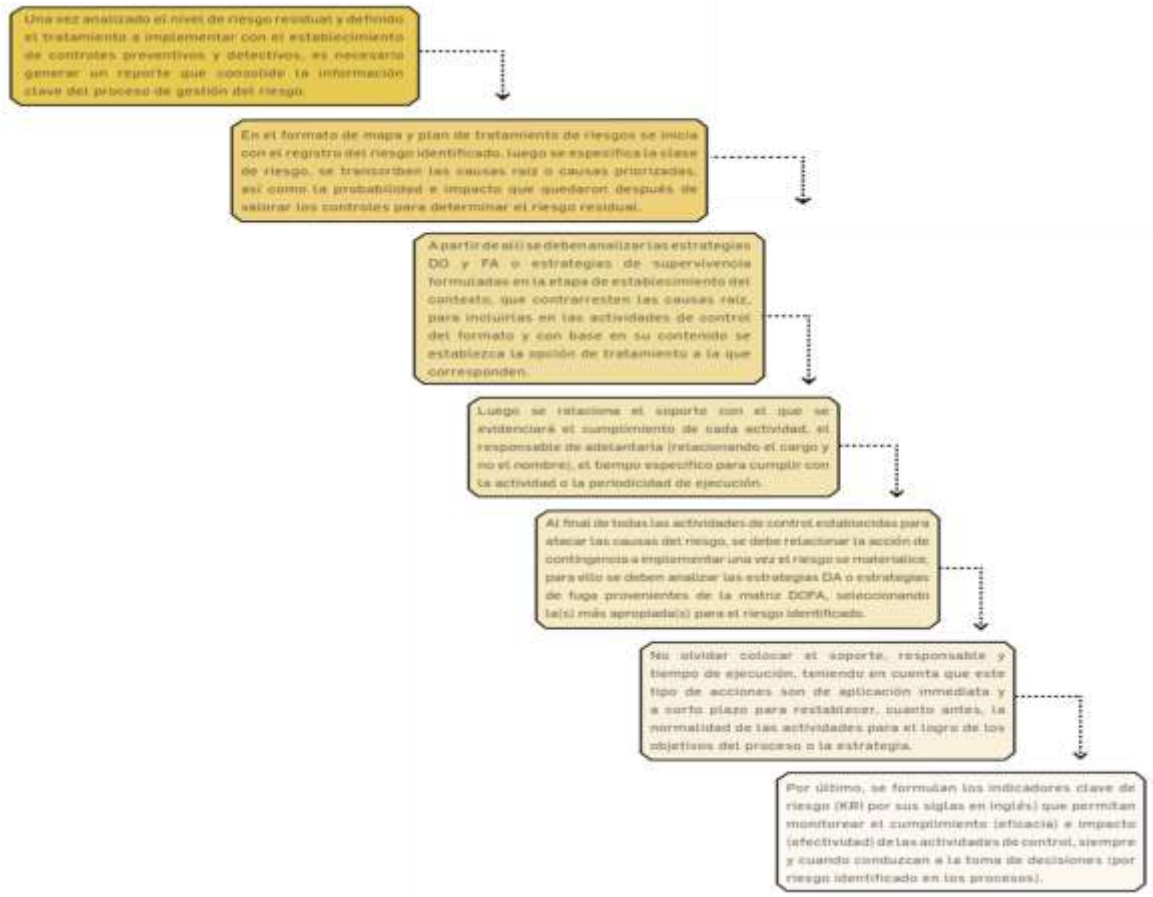
el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.	riesgos (donde existan), comités de contratación, entre otros. Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.	S.C.I. El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I.

LÍNEA ESTRATÉGICA	
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la alta dirección y el comité institucional de coordinación de control interno.	
Actividades de monitoreo y revisión a realizar	La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente: ■ Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. ■ Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. ■ Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. ■ Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ■ Hacer seguimiento y pronunciarse por lo menos cada trimestre 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. ■ Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. ■ Revisar los planes de 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.

1ª. LÍNEA DE DEFENSA	
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Está conformada por los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.	
Actividades de monitoreo y revisión a realizar	Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente: ■ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso. ■ Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. ■ Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. ■ Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ■ Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. ■ Revisar los planes de 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 y lograr el cumplimiento a los objetivos. ■ Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

	fuera del perfil de riesgo de la entidad. ■ Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. ■ Revisar los planes de 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 que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

3ª. LÍNEA DE DEFENSA	
Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. La tercera línea de defensa está conformada por la oficina de control interno o auditoria Interna.	
Actividades de monitoreo y revisión a realizar	La oficina de control interno o auditoría interna monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente: ■ Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. ■ Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. ■ Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción. ■ Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. ■ Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. ■ para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.



La Contraloría Departamental del Huila aplicará los principios aquí establecidos para todos los riesgos detectados a los que está expuesta la entidad, y los demás que sean necesarios u obligatorios institucionalizados por entidades competentes como la Presidencia de La República, el Departamento Administrativo de la Función Pública - DAFP, las normas NTC ISO, las Guías Técnicas Colombianas y todas aquellas que por mandato legal deba cumplir.