GOBERNACIÓN
Departamento Archipiélago de San Andrés,
Providencia y Santa Catalina
Reserva de Biosfera Seaflower
NIT: 892400038-2

ISO 9001:2015 BUREAU VERITAS Certification

Decreto No. 0385
(**)**

21 SEP 2021

"Por el cual se adopta la Política de Administración de Riesgos en la Gobernación del Departamento Archipiélago de San Andrés, Providencia y santa Catalina Islas".

LA SECRETARIA DE PLANEACION, en el uso de sus facultades consagradas en el decreto 371 del 14 de Septiembre de 2021.

CONSIDERANDO

Que el artículo 209 de la constitución Política establece que "La Administración Pública, en todos sus órdenes tendrá un control interno que se ejercerá en los términos que señale la ley",

Que el artículo 269 de la misma Carta Política estipula que "En las necesidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de Control Interno, de conformidad con lo que disponga la ley",

Que el parágrafo único del artículo 1° de la ley 87 de 1993, por medio de la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones, señala: El control Interno se expresará a través de las políticas aprobadas por los niveles de dirección y administración de las respectivas entidades y se cumplirá en toda la escala de la estructura administrativa, mediante la elaboración y aplicación de técnicas de dirección, verificación y evaluación de regulaciones administrativas, de manuales de funciones y procedimientos, de sistemas de información y de programas de selección inducción y capacitación de personal.

Que los literales a) y f) del artículo 2° de la ley 87 de 1993, establecieron que el diseño y desarrollo el sistema de Control Interno se orientará, entre otros, al logro de los siguientes objetivos fundamentales: a) proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten; (...) f. Definir y aplicar medidas para prevenir los riesgos detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos; (...),

Que el artículo 10 del decreto 2145 de 1999, señala: "Los elementos mismos del sistema de control interno mencionados en la ley 87 del 27 de noviembre de 1993 y demás normatividad relacionada, conforman cinco grupos que se interrelacionan y que constituyen los procesos fundamentales de la administración: Dirección, planeación, Organización, Ejecución Seguimiento y Control (Evaluación). Los responsables de fortalecer la interrelación y funcionamiento armónico de los elementos que funcionan estos cinco grupos son los servidores públicos en cumplimiento de las funciones asignadas en la normatividad vigente, de acuerdo con el área o dependencia de la cual hace parte."

Que el artículo 1° del Decreto 1537 de 2001 reglamentario de la ley 87 de 1993 establece que "Las entidades y organismos del Estado implementaran acciones para el desarrollo racional de su gestión. Para tal efecto, identificaran los procesos institucionales, de tal manera que la gestión de las diferentes dependencias de la organización, se desarrollen articuladamente en torno a dichos procesos, los cuales se racionalizaran cuando sea necesario.

Que el artículo 4° del Decreto 1537 de 2001 reglamentario de la ley 87 de 1993 dispone que "Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán políticas de administración del riesgo".

Con de la entrada en vigencia del modelo integrado de planeación y gestión (MIPG), y su actualización por medio del Decreto 1499/2017 que integra los sistemas de gestión de la calidad y de desarrollo administrativo; se crea un único sistema de gestión articulado 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. En atención a lo que establece COSO 2013 y COSO ERM 2017, los planes, programas o proyectos deben contemplar los riesgos para su ejecución y logro de sus objetivos.

Que el artículo 2.2.21.1.6 del Decreto 648 de 2017, establece como una de las funciones del comité institucional de coordinación de control interno, someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

Que el Modelo Estándar de Control Interno el cual está inmerso dentro de la 7ª. Dimensión de MIPG (componente evaluación riesgos) determinó la administración del riesgo como un componente del subsistema de control Estratégico, el cual obliga a las entidades públicas a emprender las acciones necesarias que le permitan el manejo de eventos (riesgos) que puedan afectar negativamente el logro de los objetivos institucionales. Para ello se integran cinco elementos de MECI: Ambiente de control, evaluación del riesgo, actividades de control, Información y comunicación y actividades de monitoreo. Todos estos elementos se articulan con el esquema de las líneas de defensa.

La Gobernación debe contar con una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos. Adicional a los riesgos operativos, es importante identificar los riesgos de corrupción, los riesgos de contratación, los riesgos para la defensa jurídica, los riesgos de seguridad digital, entre otros. La aceptación del riesgo puede ocurrir sin tratamiento del riesgo. Los riesgos aceptados están sujetos a monitoreo. Los riesgos de corrupción son inaceptables.

Que el Código Disciplinario Único, Ley 734 de 2002, en su Artículo 34, Numeral 31 establece entre los Deberes de todo Servidor Público: "Adoptar el Sistema de Control Interno y la función independiente de Auditoría Interna de que trata la Ley 87 de 1993 y demás normas que la modifiquen o complementen".

Que el mapa de riesgos es la herramienta conceptual y metodológica que permite identificar, analizar y valorar los riesgos e identificar las acciones prioritarias para su administración al interior de la entidad.

Que mediante el decreto 371 del 14 de Septiembre de 2021, el gobernador del departamento le otorgó la facultad de adopción de la política de administración de riesgos a la secretaria de planeación.

Que, en mérito de lo expuesto,

DECRETA

Artículo 1°. Adopción: Adoptar la Política de Administración de Riesgos, presentada por el comité Institucional de Coordinación de Control Interno de la Gobernación del Departamento Archipiélago de San Andrés, Providencia y Santa Catalina Islas, en el marco del Modelo Integrado de Planeación y Gestión MIPG v2, con el objeto de brindar un adecuado tratamiento de los riesgos de gestión institucional por procesos y proyectos de inversión, que incluya los asociados a otros sistemas de gestión, entre otros, como los de sistema Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el trabajo, de Gestión Ambiental, de Seguridad de la Información, procesos de selección y/o contratación, de la defensa jurídica y los posibles riesgos relacionados con actos de corrupción para garantizar el cumplimiento de la

misión, visión y objetivos institucionales, el cual se describe en el anexo que hace parte integral del presente Decreto.

Artículo 2°. Incumplimiento El incumplimiento de las disposiciones del artículo primero, por parte de los servidores públicos de la entidad será sancionado de conformidad con lo establecido en el Código Disciplinario único.

Artículo 3°: Divulgación. La política de Administración de Riesgos y su resultado Mapa de Riesgos se divulgarán a todos los servidores de la entidad y se mantendrán en la red interna, para su permanente consulta.

Vigencia y derogatoria. El presente decreto deroga en su totalidad el Decreto No. 398 del 2012 y el presente rige a partir de la fecha.

POLÍTICA DE OPERACIÓN DE RIESGOS

La Gobernación Departamental define su política de administración de riesgos atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles, en entidades públicas del DAFP 2018, articulada con el Modelo Integrado de Planeación y Gestión (MIPG v2).

Todos los procesos y dependencias contando con la participación activa de los servidores públicos responsables de los procesos, planes y proyectos deben identificar, analizar, valorar, administrar y controlar los riesgos asociados a sus respectivos procesos, con el fin de minimizar aspectos adversos ante una desviación o eventualidad que impida dar continuidad a la gestión institucional o cumplir con los compromisos adquiridos con los grupos de valor.

Para administrar adecuadamente los riesgos la Administración Departamental acata la metodología propia y determina las acciones para:

- **Asumir un riesgo** (ningún caso de corrupción podrá ser aceptado): Aceptar la existencia del riesgo debido a que se encuentra en una zona de riesgo "Baja" o "Moderada"; el responsable puede aceptar las posibles consecuencias, si estas no afectan el logro de los objetivos del proceso y debe elaborar los planes de contingencia para su manejo. Para riesgos que no tienen una opción de tratamiento inmediata y no pueden ser evitados, se debe generar un análisis por parte de del Líder del Proceso o jefe de la Dependencia para revisar su aceptación; estos riesgos deben permanecer en constante monitoreo y deben contar con planes de contingencia para actuar en caso de materializarse.
- **Reducir el riesgo:** Implementar acciones encaminadas a reducir el nivel de riesgo, bien sea mejorando controles existentes o implementando nuevos controles.
- **Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
- **Compartir el riesgo:** Tomar acciones encaminadas a trasladar el impacto o la probabilidad del riesgo, o una parte, a un tercero a través de pólizas o tercerización de servicios, entre otros.

OBJETIVOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

GENERAL

Fortalecer el diseño y la implementación de la política de Administración del Riesgo a través del adecuado y oportuno tratamiento de los riesgos para garantizar el cumplimiento de la misión y objetivos institucionales de la Gobernación del Departamento Archipiélago de San Andrés, Providencia y santa Catalina Islas.

ESPECIFICOS

- Establecer disposiciones y criterios institucionales que orienten a la Gobernación de San Andrés Islas en la correcta identificación, análisis, valoración y administración de los riesgos, que pueden afectar de forma positiva o negativamente el logro de los objetivos institucionales en el marco de los procesos, proyectos y planes.
- Generar una visión sistémica acerca de la administración y evaluación de riesgos, consolidando un ambiente de control adecuado y un direccionamiento estratégico, que fije orientación clara y planeada de la gestión suministrando las bases para el adecuado desarrollo de la Actividad de Control.
- Consolidar el ambiente de control necesario para la entidad y el direccionamiento estratégico, que fije la orientación clara y planeada de la gestión de los riesgos, como fundamento para el adecuado desarrollo de las actividades de control.
- Reducir la vulnerabilidad y fortalecer la prevención y mitigación de los efectos de los riesgos.
- Proteger los recursos de la entidad, resguardándolos de la materialización de los riesgos.
- Declarar el compromiso por parte de todos los servidores de la Administración Departamental y de los particulares que cumplan funciones públicas en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.

Alcance de la Política

La política de riesgos es aplicable a todos los procesos, programas y proyectos de la Gobernación y a todas las acciones ejecutadas por los servidores durante el ejercicio de sus funciones y en representación de la entidad.

Términos y Definiciones

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicio web, redes hardware, información física o digital, recurso humano, entre otros, que utiliza la organización par a funcionar en el entorno digital.
- **Administración del Riesgo:** Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.
- **Análisis de Riesgos:** Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.
- **Amenazas:** causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Actividades de control:** 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.
- **Apetito al riesgo:** Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización del riesgo.
- **Consecuencias:** Hechos o acontecimientos que se derivan o resultan de la ocurrencia o la materialización de un riesgo, que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Corrupción:** Uso del poder para desviar la gestión de lo público hacia el beneficio privado.
- **Causas:** Medios, circunstancias, situaciones o agentes generadores del evento.

- **Control:** Acciones encaminadas a reducir la probabilidad de ocurrencia o el impacto que pueda generar la materialización del riesgo. (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Evento:** Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo, tiene relación directa con las actividades críticas de los planes operativos, las actividades de ruta crítica de los Proyectos de Inversión y las actividades críticas de control de los procesos.
- **Frecuencia:** Periodicidad con que ha ocurrido un evento.
- **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.
- **Gestor del Riesgo:** funcionario líder de la dependencia, quien apoya al responsable del riesgo.
- **Identificación del Riesgo:** Descripción de la situación no deseada.
- **Impacto:** Magnitud de las consecuencias que pueden ocasionar a la entidad la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.
- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Políticas de manejo del Riesgo:** Son los criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar, los riesgos en la entidad, en función de su evaluación.
- **Probabilidad:** La posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.
- **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.
- **Responsable del riesgo:** Es el encargado de identificar, valorar y definir el plan de contingencia, el manejo y monitoreo para cada uno de los riesgos del proceso bajo su responsabilidad.
- **Riesgo:** Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.
- **Riesgo residual:** Nivel del riesgo que permanece luego de tomar medidas de tratamiento del riesgo.
- **Riesgo Inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad de impacto.
- **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 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 aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.
- **Tratamiento:** Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

- **Tolerancia al riesgo:** Son los niveles aceptables de desviación relativa a la consecuencia de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes.
- **Valoración:** Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.
- **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
- **CGDC:** comité de gestión y desempeño institucional.
- **CICI:** Comité Institucional de control Interno.

Compromisos, Roles y Responsabilidades frente al Riesgo

Es importante tener claro el esquema de responsabilidades integrada por el esquema de "Líneas de Defensa", que proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.

Estas líneas ayudan a tener un modelo claro de iniciativas de gestión del riesgo. Las responsabilidades de la gestión de riesgos y del control están distribuidas en varias áreas y no se concentra en la oficina de Control Interno de Gestión; de allí que deban ser coordinadas cuidadosamente para asegurar que los controles operen.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Estratégica	Alta Dirección, CGDI, CICI	• Establecer la Política del riesgo • Promover y cumplir los estándares de conducta e integridad del servidor público • Realizar seguimiento y análisis periódico a los riesgos institucionales
Primera Línea	Líderes de Proceso	• Asegurar que se identifiquen los riesgos y establecer actividades de control a los procesos, proyectos y productos en cada vigencia • Realizar seguimiento y análisis a los controles de los riesgos según la periodicidad establecida • Actualizar el mapa de riesgos del proceso a cargo cuando se requiera. Tratándose de riesgos de corrupción los líderes de los procesos y sus equipos adelanta un Monitoreo y revisión.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Segunda Línea	Supervisores y Servidores Públicos delegados	•Análisis de los objetivos de la entidad tanto en el orden estratégico como de procesos. • Hacer seguimiento y reportar en el SGI los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. • Aplicar los estándares de conducta e integridad en sus funciones.
	Oficina Asesora de Planeación	• Asesorar en la identificación de los riesgos institucionales • Acompañar y orientar a los procesos sobre la metodología para la identificación, análisis, calificación y valoración del riesgo • Consolidar el Mapa de riesgos institucional y presentarlo para seguimiento ante el CGDI • Liderar la elaboración y consolidación de los mapas de riesgos por proceso. Tratándose de riesgos de corrupción las oficinas de Planeación adelantan un Monitoreo y revisión.

Tercera Línea	Oficina de Control interno	• Asesorar en la identificación de los riesgos institucionales • Analizar el diseño e idoneidad de los controles establecidos en los procesos • Realizar seguimiento a los riesgos consolidados en los mapas de riesgos • Adelantar seguimiento a riesgos de corrupción

Esta política apoya el fortalecimiento de los cinco componentes a partir del desarrollo de otras dimensiones como Direccionamiento Estratégico y Planeación, Gestión con Valores para resultados y Talento Humano, y de allí de la transversalidad de las actividades:

DIMENSIÓN	ACTIVIDADES POR IMPLEMENTAR	LINEA DE DEFENSA RESPONSABLE	ASPECTOS POR EVALUAR DENTRO DEL SISTEMA DE CONTROL INTERNO
Direccionamiento Estratégico y Planeación	Dado que en esta dimensión se define la ruta organizacional que debe seguir la entidad para lograr sus metas, resultados, y en general sus objetivos, se deben emitir los lineamientos para crear un ambiente favorable al control y para la administración del riesgo. En esta dimensión, se identifican los riesgos, se diseñan los controles para que la gestión eficiente, efectiva y transparente, y se tenga una adecuada prestación de servicios o producción de bienes.	Línea Estratégica	• Evaluación de la Política de riesgos • Monitoreo permanentemente los riesgos de corrupción. • Monitoreo al estado de los riesgos aceptados (apetito por el riesgo), con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad. • Avance en el esquema de líneas de defensa
Direccionamiento Estratégico y Planeación Gestión para resultados	Así mismo se deben establecer líneas de reporte dentro de la entidad para el funcionamiento del Sistema de Control Interno. Cada líder suministra información de forma periódica, con datos y hechos que le permitan la toma de decisiones a la alta dirección	Línea Estratégica	• Informes de evaluación a los aspectos clave definidos a partir del Esquema de líneas de Defensa.
Gestión para resultados	A partir de la dimensión se asegura que la estructura organizacional, los procesos de la cadena de valor y los de apoyo, la asignación del talento humano a los proyectos, programas o procesos, el uso de los bienes muebles e inmuebles, el suministro de servicios internos, la ejecución presupuestal y la focalización de los recursos, estén en función	Línea Estratégica	• Mejoras en la prestación del servicio (evaluaciones sobre percepción de los usuarios). • Informes de evaluación a los aspectos clave definidos a partir del Esquema de líneas de Defensa.

	del cumplimiento de los propósitos de la entidad y de atender lo previsto en la planeación institucional, de forma eficiente		
Gestión del Talento Humano	Es necesario que una adecuada GETH asegure que la selección, la capacitación, la evaluación del desempeño y la calidad de vida laboral, se conviertan en herramientas adecuadas para el ejercicio de las funciones y responsabilidades y en condición óptima, facilitando el autocontrol por parte de cada servidor. La adecuada GETH debe igualmente contemplar las directrices para la toma de decisiones frente al talento humano, en especial sobre aquellos aspectos que tienen que ver con su preparación y responsabilidad frente al Sistema de Control Interno, y sobre los parámetros éticos y de integridad que han de regir todas las actuaciones de los servidores públicos.	Línea Estratégica	• Aplicación y cumplimiento código de integridad. • Clima laboral • Temas Disciplinarios • Impacto del Plan Institucional de Capacitación PIC

Establecimiento del contexto.

Definición de los parámetros internos y externos que se han de tomar en consideración con la administración del riesgo. A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

Se determinan las características o aspectos esenciales:

Establecimiento del contexto externo	**Establecimiento del contexto proceso**	**Establecimiento del contexto interno**
Del entorno en el cual opera la entidad. Se pueden considerar factores como: • Políticos • Sociales y Culturales • Legales y reglamentarios • Tecnológicos • Financieros	Del proceso y sus interrelaciones. Se pueden considerar factores como: • Objetivo del proceso • Alcance del proceso • Interrelación con otros procesos • Procedimientos asociados • Responsables del proceso	Del ambiente en el cual la organización busca alcanzar sus objetivos. Se pueden considerar factores como: • Estructura organizacional • Funciones y responsabilidades • Políticas, objetivos y estrategias implementadas • Recursos y conocimientos con que se cuenta (personas, procesos, sistemas,

• Económicos		tecnología) • Relaciones con las partes involucradas • Cultura organizacional.

Fuente: Función Pública, 2017

La Administración Departamental con el fin de reflejar un panorama que le permitiera establecer los diferentes factores de riesgos relacionados con los contextos externos e internos a los cuales está expuesta la Entidad, realizó un proceso de compilación y análisis de las condiciones en las que se encontraba tanto el territorio como la misma Entidad en cada uno de los sectores de manera integral (sectoriales, transversales y poblacionales).

Para la elaboración del diagnóstico se tuvieron en cuenta los siguientes pasos:

- Análisis inicial para el cierre de brechas.
- Lectura sectorial y transversal del territorio.
- Identificación de problemas.
- Definición de causas y consecuencias.
- Ejercicio participativo con la comunidad.
- Síntesis de la situación actual del territorio.

Del mismo modo se realizó un análisis al estado interno de la entidad en cuanto a medir el desempeño Institucional evidenciando un bajo cumplimiento en el grado de implementación de las políticas establecidas en el modelo Integrado de Planeación y Gestión – MIPG en especial en las dimensiones de talento humano y gestión del conocimiento.

En consecuencia la Entidad ha identificado y constituido con responsabilidad una línea base, que se convierte en oportunidades de mejora para la implementación de las 17 políticas del MIPG.

En cuanto al contexto de proceso y el contexto interno la Administración adelantó con la ESAP el convenio 758 de 2018 "Estudio técnico de rediseño institucional de la Gobernación Archipiélago de San Andrés y Providencia y Santa Catalina", entregado en julio de 2019, el cual permitió avanzar en el estudio de cargas laborales. Se trata de un avance para fortalecer el proceso de modernización de la Administración, a través de estrategias de rediseño administrativo, mejoramiento de la gestión del talento Humano, aplicación de tecnología de la información, fortalecimiento de la capacidad de gestión de la Entidad, adecuación de la planta física y todo lo requerido para minimizar los factores de riesgo que se puedan presentar en todos los procesos.

Metodología para la administración del riesgo:

Se realiza determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. 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 al desarrollo del proceso.

¿Qué consecuencias tendría su materialización? Determinar los posibles efectos por la materialización del riesgo. En la descripción del riesgo se deben tener en cuenta las respuestas a las preguntas anteriormente enunciadas.

Riesgo de corrupción:

Se establecen sobre procesos. El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos. Para facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción se

utilizará la siguiente matriz que incorpora cada uno de los componentes de su definición. Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción:

MATRIZ DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	Acción u Omisión	Uso del poder	Desviar la gestión de lo publico	Beneficio Privado

Fuente: Secretaría de Transparencia de la Presidencia de la República

Análisis del Riesgo

Busca determinar el grado en el cual se puede materializar un riesgo, para esto se tienen en cuenta la probabilidad e impacto del riesgo "Riesgo Puro" es decir, sin considerar los controles existentes para evitar que este riesgo se materialice.

Análisis de la probabilidad:

Se analiza que tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

	FRECUENCIA DE LA ACTIVIDAD	TABLA PROBABILIDAD
MUY BAJA	La actividad se realiza 2 veces por año.	20%
BAJA	La actividad se realiza mínimo 3 veces al año y máximo 24 veces al año.	40%
MODERADA	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%
ALTA	La actividad se realiza mínimo 500 veces al año y máximo 5000 veces al año.	80%
	La actividad se realiza 5000 veces o más al año.	100%

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los servidores que desarrollan el proceso y de sus factores internos y externos.

Análisis del Impacto:

El impacto se basa en la siguiente tabla, considerando la pérdida reputaciones y económica.

Criterios para calificar el impacto – riesgos de gestión

	Pérdida Económica	Pérdida Reputacional
Insignificante- 20%	Perdidas menores a 10 SMLMV.	Sólo de conocimiento de algunos funcionarios.
Menor- 40%	Mayores o iguales a 10 SMLMV y menores a 21 SMLMV.	De conocimiento general de la entidad a nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado- 60%	Mayores o iguales a 21 SMLMV y menores a 318 SMLMV.	Afecta imagen con algunos clientes que impacten significativamente los objetivos.
Mayor- 80%	Mayores o iguales a 318 SMLMV y menores a 2120 SMLMV.	Deterioro de imagen a nivel nacional, con efecto publicitario sostenido a nivel país.
	Mayores a 2120 SMLMV.	Deterioro de imagen a nivel internacional, con efecto publicitario sostenido a nivel internacional.

Fuente: DAFP - Adaptado de curso Riesgo Operativo Universidad del Rosario 2020

NOTA: Si se tienen para un mismo riesgo ambos impactos (reputacional y económico) que tienen diferentes niveles se toma el más alto.
Ej.: Para un mismo riesgo se tiene impacto económico en nivel Insignificante y reputacional en nivel mayor, se tomaría las reputaciones que es el de más impacto. En la redacción del riesgo se hará énfasis en este último.

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.

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
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.

NOTA: La entidad deberá adaptar los criterios a su realidad. El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Severidad

- ✓ Nivel de un riesgo, dado por una probabilidad y un impacto.
- ✓ En cada nivel se define el tratamiento y los niveles de responsabilidad.

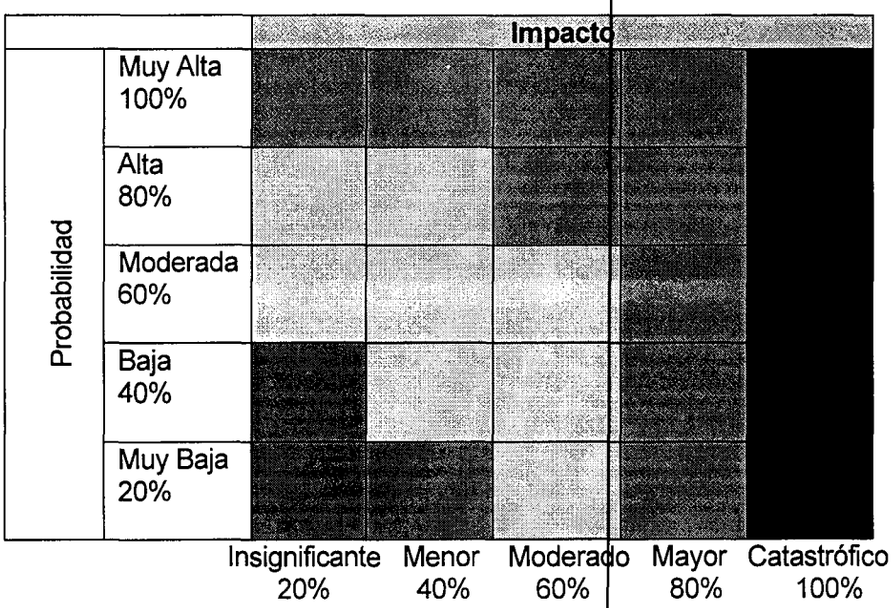
		Impacto				
		Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Probabilidad	Muy Alta	Alto	Alto	Alto	Alto	Extremo
	Alta	Moderado	Moderado	Alto	Alto	Extremo
	Media	Moderado	Moderado	Moderado	Alto	Extremo
	Baja	Bajo	Moderado	Moderado	Alto	Extremo
	Muy Baja	Bajo	Bajo	Moderado	Alto	Extremo

Fuente: Adaptado de curso Riesgo Operativo Universidad del Rosario 2020

	Descripción
Extremo	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, la Alta Dirección. Debe establecer el tratamiento e informar al Comité Institucional de Coordinación de Control Interno.
Alto	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe establecer el tratamiento e informar al Comité Institucional de Gestión y Desempeño.
Moderado	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe hacer seguimiento mediante procedimientos existentes.
Bajo	Los riesgos que se ubiquen en esta zona serán aceptados, el líder del proceso debe hacer seguimiento y llevar el registro correspondiente.

Fuente: Adaptado de curso Riesgo Operativo Universidad del Rosario 2020

Mapa de Calor



Fuente: Adaptado de curso Riesgo Operativo Universidad del Rosario 2020

Nota Importante: Frente al análisis de probabilidad e impacto no se utiliza criterio de experto, se deben aplicar las tablas bajo los criterios establecidos, tanto para probabilidad como impacto.

Análisis de Impacto en Riesgos de Corrupción:

El análisis del impacto se realizará teniendo en cuenta solamente los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos; por lo tanto, no aplican los niveles de insignificante y menor que si aplican en los demás riesgos.

Criterios para calificar el impacto – Riesgo de Corrupción

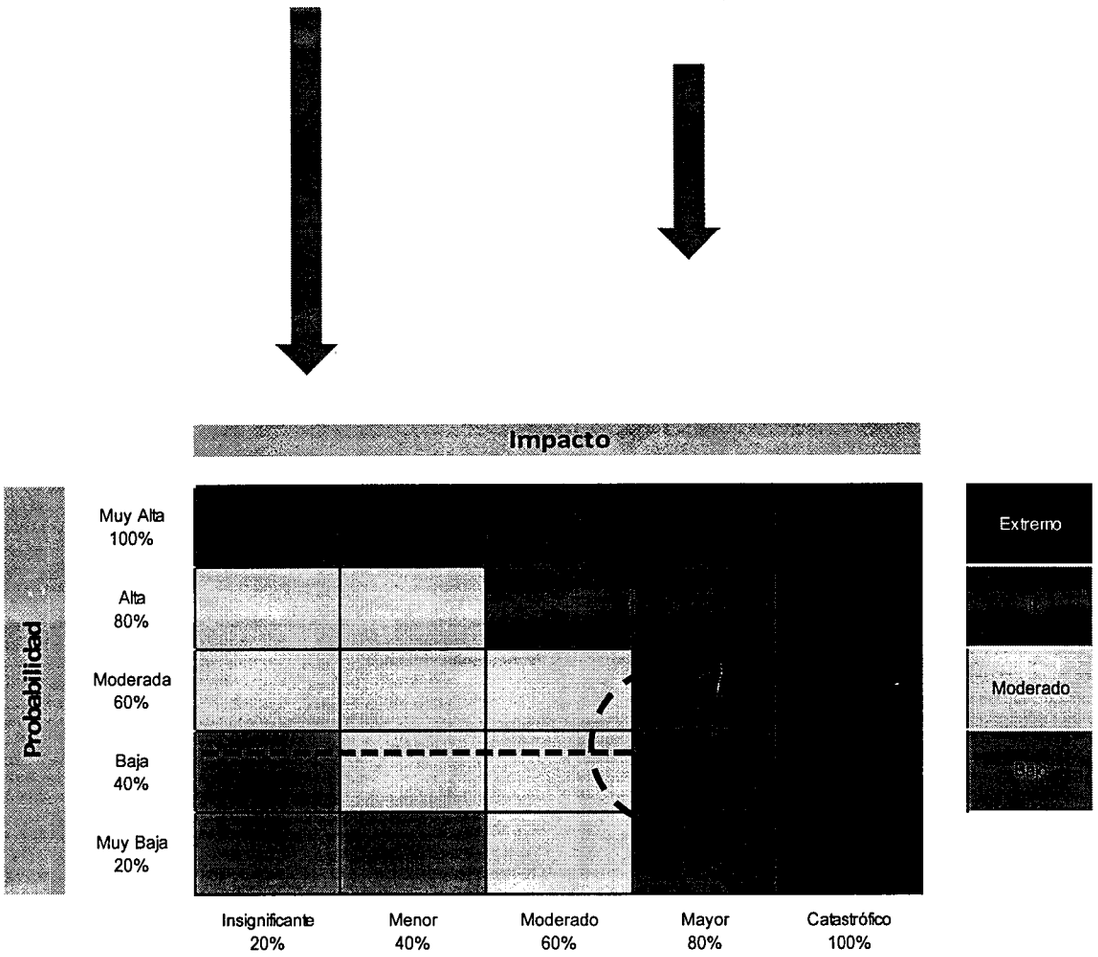
	Pregunta: Si el riesgo de corrupción se materializa podría...	SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de los servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicio o los recursos públicos?		
9	¿Generar perdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la fiscalía, u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad en el sector?		
16	¿Ocasionar lesiones físicas o pérdidas de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNO a CINCO preguntas (s) genera un impacto MODERADO Responder afirmativamente de SEIS a ONCE preguntas genera un impacto MAYOR Responder afirmativamente de DOCE a DIECIOCHO preguntas genera un impacto CATASTROFICO.			
	Genera medianas consecuencias sobre la entidad		
	Genera altas consecuencias sobre la entidad		
	Genera consecuencias desastrosas para la entidad		

Calificación del riesgo inherente, antes de controles:

Esta se logra a través de la estimación de la probabilidad y el impacto que puede causar la materialización del riesgo, de acuerdo con el siguiente gráfico:

	Frecuencia de la Actividad	Tabla Probabilidad
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%
Baja	La actividad se realiza mínimo 5 veces al año y máximo 12 veces al año.	40%
Moderada	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%
Alta	La actividad se realiza mínimo 365 veces al año y máximo 3660 veces al año.	80%
Muy Alta	La actividad se realiza 3661 veces o más al año	100%

	Pérdida Económica	Pérdida Reputacional
Insignificante-20%	Perdidas menores a 10 SMLMV.	Sólo de conocimiento de algunos funcionarios.
Menor-40%	Mayores o iguales a 10 SMLMV y menores a 21 SMLMV	De conocimiento general de la entidad a nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado- 60%	Mayores o iguales a 21 SMLMV y menores a 318 SMLMV	Afecta imagen con algunos clientes que impacten significativamente los objetivos.
Mayor- 80%	Mayores o iguales a 318 SMLMV y menores a 2120 SMLMV	Deterioro de imagen a nivel nacional, con efecto publicitario sostenido a nivel país
Catastrófico- 100%	Mayores a 2120 SMLMV	Deterioro de imagen a nivel internacional, con efecto publicitario sostenido a nivel internacional



Fuente: Departamento Administrativo de la Función Pública DAFP

Ejemplo: proceso de contratación

Riesgo: Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

1. La actividad de contratos implican 10 en el mes = 120 contratos en el año (Probabilidad "Moderada" = 60%).

2. De llegar a materializarse tendría pérdida económica de 500 SMLMV (Impacto "Mayor" =80%)

Riesgo Inherente = Probabilidad Moderada 60%,
Impacto Mayor 80%
Nivel Severidad: Alta

Controles:

Medidas que permite reducir o mitigar un riesgo.

- ✓ La identificación de controles se debe realizar para cada riesgo a través de las

entrevistas con los líderes de los procesos y servidores responsables.

- ✓ Los responsables de implementar y monitorear los controles son los líderes de los procesos y servidores responsables.

Se orientan a prevenir y detectar la materialización de los riesgos. Su efectividad depende, de que tanto se están logrando los objetivos estratégicos y de proceso de la entidad.

Las actividades de control, independiente de la tipología de riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo de origine, o en caso de que se presente, sea detectada de manera oportuna.

Responsable de ejecutar el control: Identifica el cargo del servidor que ejecuta el control, en caso se ser controles automáticos se identificará el sistema que realiza la actividad.

Acción: Se determina mediante verbos en los cuales se identifica la acción a realizar como parte del control.

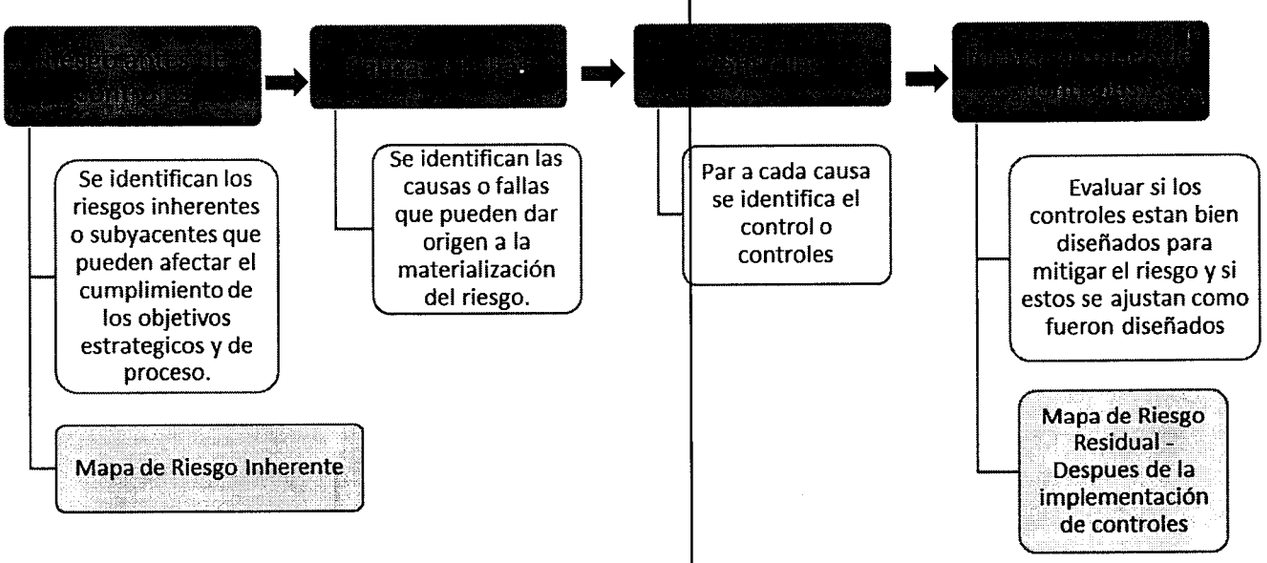
Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del control.

Clasificación de los controles:

Los controles están clasificados en dos grupos según su atributo (atributos de eficiencia y atributos de formalización). Los controles con atributo de **Eficiencia** tienen las siguientes características:

De acuerdo con la forma como se activa el control tenemos **(Tipos de controles)**,

- **Controles Preventivos:** Están diseñado para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.
- **Controles Detectives:** Controles que están diseñado para identificar un evento o resultado no previsto después de que se haya producido. Busca detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.
- **Correctivo: (Después)** Acción que se ejecutan después de que se materializa el riesgo y en la mayoría de las ocasiones permiten reducir el impacto de dicho riesgo.



De acuerdo con la forma en que se ejecutan **(Implementación)** tenemos,

- **Manual:** Controles que son ejecutados por una persona., tiene implícito el error humano.

Ejemplo: El profesional de Talento Humano verifica la información generada por el sistema biométrico para establecer el cumplimiento por parte del personal, en el número de horas determinadas para el otorgamiento del descanso remunerado establecido en abril y diciembre de cada vigencia.

- **Automático:** Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.

Ejemplo: El sistema biométrico valida el ingreso del personal y visitantes del edificio, para evitar el acceso no autorizado a las instalaciones de la entidad.

Los controles con atributo de **Formalización** tienen las siguientes características:

Documentación

- **Documentado:** Identifica los controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujo gramas o cualquier otro documento propio del proceso.
- **Sin Documentar:** Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.

Frecuencia:

- **Continuo:** Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.
- **Aleatorio**: Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo.

Evidencia:

- **Registro Sustancial**: Corresponde a la evidencia de la ejecución del control, que es verificable y no manipulable por parte del usuario. Ejemplo: Log de auditoria de un sistema, cartas con firma mecánica, firmas digitales, actas de Juan o Comités, firma de asistencia a capacitaciones.
- **Registro Material**: Corresponde a la evidencia de la ejecución del control, que es verificable, pero podría ser manipulable por parte del usuario. Ejemplo: correos electrónicos, vistos buenos y documentos electrónicos sin seguridad.
- **Sin Registro**: Son aquellos controles que se ejecutan, pero al validar algún tipo de evidencia de su ejecución no es posible determinarla.

Tabla de Valoración de los controles

Los controles se valoran de acuerdo con su atributo, solamente los atributos de Eficiencia tendrán valoración, los atributos de Formalización se recogerán de

manera informativa, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad.

Características			**Peso**
Atributos de Eficiencia	Tipo	Preventivo	49%
		Detective	33%
		Correctivo	16%
Formalización	Implementación	Automático	49%
		Manual	25%
	Documentación	Documentado	-
		Sin Documentar	-
	Frecuencia	Continua	-
		Aleatoria	-
	Evidencia	Registro Sustancial	-
		Registro Material	-
		Sin registro	-

Variables a tener en cuenta para el adecuado diseño de Controles:

Al momento de definir si un control o lo controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción de este las siguientes variables:

Paso	**Variable**	**Características**	**Observaciones**
1	Debe tener definido el responsable de realizar la actividad de control	Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes funcionarios para así reducir el riesgo de error o de actuación es irregulares o fraudulentas. Si ese responsable quisiera hacer algo indebido, por sí solo, no lo podrá hacer. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de la ejecución.	El control debe iniciar con un claro responsable o un sistema de aplicación. Ej.: (El profesional de Contratación..., El sistema SECOP II...) Evitar colocar áreas de manera general o nombres de personas. El control debe estar asignado a un cargo específico.
		Diario, mensual, trimestral, anual, etc.	No debe quedar a

2	Debe tener una periodicidad definida para su ejecución	Su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la prioridad se debe evaluar si este previene o detecta de manera oportuna el riesgo.	criterio la prioridad de la realización del control ya que se tendría problema en el diseño del control. (El auxiliar de cartera mensualmente..., El sistema xxx cada vez que se va a realizar el pago.)
3	Debe indicar cuál es el propósito del control	Debe indicar para que se realiza el control, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar), o detectar la materialización del riesgo y conlleve a que se realicen los ajustes y correctivos en el diseño del control o en su ejecución.	Ej.: El auxiliar de cartera mensualmente verifica que los valores recaudados en banco correspondan con los a los adeudados por los clientes.
4	Debe establecer el cómo se realiza la actividad de control	El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo.	Ej.: El auxiliar de cartera mensualmente verifica que los valores recaudados en banco correspondan con los a los adeudados por los clientes, extractando la información directamente del portal bancario del extracto y generando el auxiliar contable de cuentas por cobrar del aplicativo, identificando las cuentas por cobrar pendientes de pago que fueron canceladas según extracto bancario
5	Debe identificar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control	Si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, debería gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observadas. Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones, o la actividad continua a pesar de indicar esas observaciones o desviaciones, el control tendría problemas en su diseño.	Ej.: El auxiliar de cartera mensualmente verifica...canceladas según extracto bancario. En caso de observar cuentas de cobro que a la fecha no se ha recibido el pago, lista las cuentas pendientes de pago y realiza llamadas a los clientes y solicita que le indiquen la fecha para el pago oportuno de los mismos.
6	Debe dejar evidencia de la ejecución de control	Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecuto el control, y se pueda evaluar que el control	Ej.: El auxiliar de cartera mensualmente verifica... para el pago oportuno de los mismos. Como

		realmente fue ejecutado de acuerdo a los parámetros establecidos en los 5 primeros pasos enunciados anteriormente.	evidencia queda listado de cuentas por cobrar pendientes de pago en Excel con los compromisos acordados con los clientes y extracto bancario.

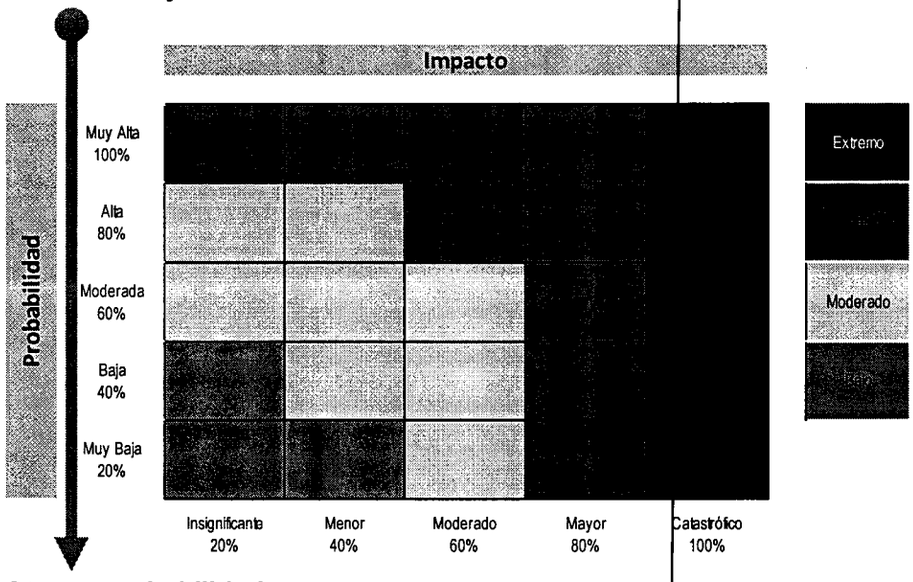
Para la adecuada mitigación de los riesgos, no basta con que un control este bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó, por qué un control que no se ejecute, o un control que se ejecute y este mal diseñado, no va a contribuir con la mitigación del riesgo.

Desplazamiento en la Matriz a partir de los Controles

Se identifica si los controles reducen la probabilidad o el impacto, para así reducir porcentualmente cada variable.

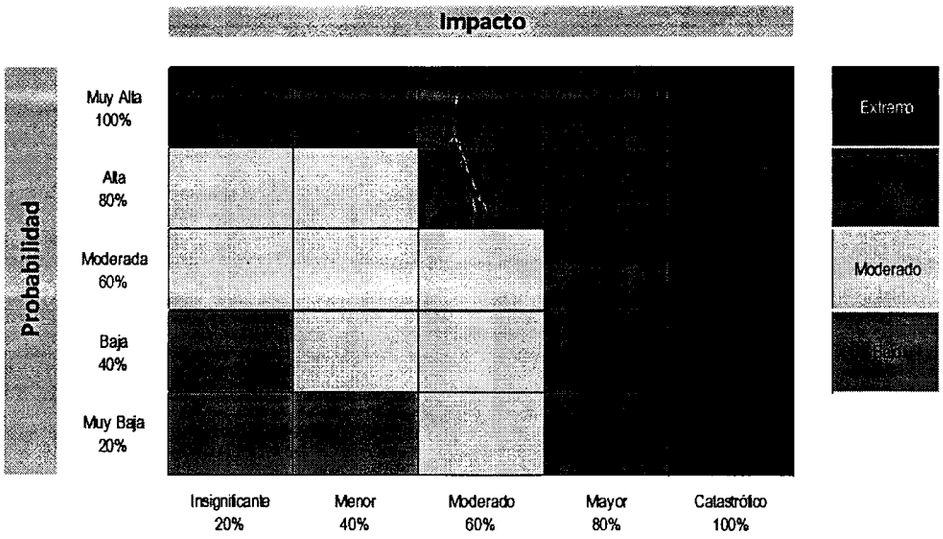
Controles Correctivos → **Atacan Impacto**

Preventivos y Detectives

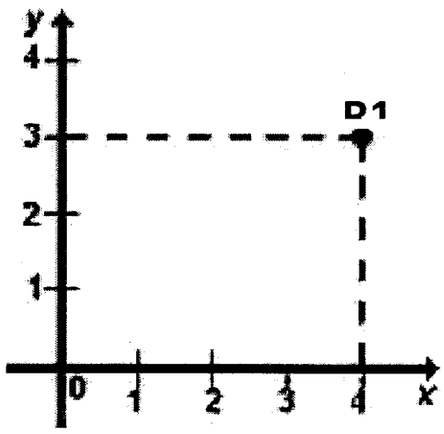


Atacan probabilidad

Detrás de esta matriz tenemos un plano cartesiano que cruza 2 ejes X y Y, ubicando un punto de riesgo.



El movimiento no es diagonal, para ir de una zona extrema a una baja, se da sobre los ejes, lo que requiere controles tanto para probabilidad como para impacto de forma individual.



El resultado de aplicar la efectividad de los controles al riesgo inherente nos determina el riesgo residual. La fórmula es la siguiente:

RIESGO INHERENTE – CONTROLES = RIESGO RESIDUAL

Dependiendo del nivel de severidad en que se ubique el riesgo residual, se da prioridad a la atención de estos, así como definir su tratamiento y las acciones a seguir.

Nota: La entidad deberá implementar en el marco de su gestión del riesgo una política de reducción máximo del 50%, para evitar que un solo control baje mucho el nivel del riesgo

(Ejemplo: Control = preventivo (49%) + automático (49%) = 98%).

La metodología establece que los controles mitigan el riesgo de forma acumulativa. Opera una política de reducción máxima del 50% para los controles.

R. RESIDUAL = R. INHERENTE – (R.I. * CONTROL)

El Riesgo Inherente tiene dos valores, uno de probabilidad y otro de Impacto.

Ejemplo Proceso de Contratación: Probabilidad Moderada 60%, Impacto Mayor 80%, Nivel Severidad: Alta.

Análisis del Control de acuerdo con la tabla de Atributos

Características			Peso
Atributos de Eficiencia	Tipo	Preventivo	49%
		Detectivo	33%
		Correctivo	16%
	Implementación	Automático	49%
		Manual	25%
Formalización	Documentación	Documentado	-
		Sin Documentar	-
	Frecuencia	Continua	-
		Aleatoria	-
	Evidencia	Registro Sustancial	-
		Registro Material	-
		Sin registro	-

1. Preventivo =49%
2. Manual = 25%
3. Documentado= si
4. Frecuencia= Continua
5. Registro sustancial

Ejemplo: El profesional de Contratación, verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor.

Cálculo para los Controles

La metodología debe establecer que los controles mitigan el riesgo de forma acumulativa. Opera una política de reducción máxima del 50% para los controles.

Ejemplo: proceso de contratación

Riesgo: Posibilidad de pérdida económica por multa y sanción del ente regulador debido a adquisición de bienes y servicios fuera de los requerimientos normativos.

Riesgo Inherente:

¿De dónde sale este valor?
De la Tabla de atributos del control

Probabilidad Moderada 60%,
Impacto Mayor 80%
Control 1 (Probabilidad)= 74% Aplico política de reducción = 37%
Control 2 (Probabilidad)= 98% Aplico política de reducción = 49%

Control 3 (Impacto)= 82% Aplico política de reducción = 41%

Continuando con el mismo ejemplo tenemos 2 Controles de Probabilidad y 1 de Impacto:

Riesgo Inherente
Probabilidad Moderada 60%,

C1 (probabilidad)= 37%
60%* 37% = 22.2
60% - 22,2% = 37,8%
C2 (Probabilidad)= 49%

37,8% * 49% = 18,52%
37,8% -18,52%= 19,28%
Probabilidad Residual= 19,28%

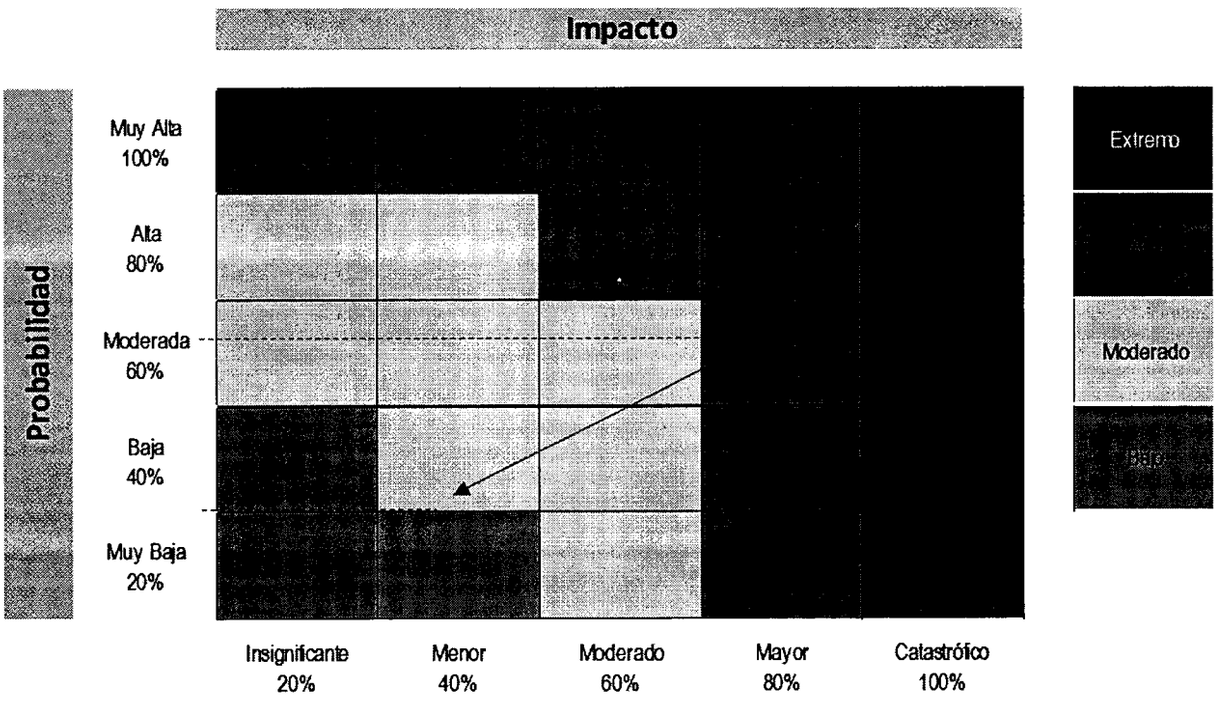
Riesgo Inherente:
Impacto Mayor 80%

C3 (Impacto)= 41%
80%* 41% = 32,8%
80%- 32,8% = 47,2%
Impacto Residual= 47,2%

Como resultado del anterior ejercicio tenemos,

Riesgo Residual = Probabilidad Muy baja 19,28 % - Impacto Moderado 47,2%
Nivel Severidad: Moderada

La metodología acumulativa busca reducir los niveles de probabilidad e impacto residual, teniendo en cuenta la eficiencia del control. La nueva ubicación del riego quedaría de la siguiente manera:



Accionar ante los riesgos materializados:

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	Líder de Proceso	**1.** Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado. **2.** De considerarlo necesario, realizar la denuncia ante el ente de control respectivo. **3.** Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento **4.** Realizar el análisis de causas y determinar acciones preventivas y de mejora. **5.** Analizar y actualizar del mapa de riesgos.
	Oficina de Control Interno	**1.** Informar al Líder del proceso de Evaluación Independiente sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. **2.** Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. **3.** Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de procesos. 4. Sugerir que se realice un plan de mejoramiento.
Riesgos de Proceso/Proyecto /Producto **(Zona Extrema, Alta y Moderada)**	Líder de Proceso	**1.** Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento de este (si es el caso), documental en el Plan de mejoramiento. **2.** Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso. **3.** Analizar y actualizar el mapa de riesgos. **4** informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.
Riesgos de Proceso/Proyecto /Producto **(Zona Baja)**	Líder de Proceso	Establecer acciones correctivas al interior de cada proceso a cargo del líder respectivo y verificar la calificación y ubicación del riesgo.
Riesgos de Proceso/Proyecto /Producto **(Zona Extrema, Alta y Moderada)**	Oficina de Control Interno	**1.** Informar al líder del proceso sobre el hecho encontrado. **2.** Orientar al líder del proceso para que realice la revisión, análisis y acciones correspondientes para resolver el hecho. **3.** Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente.
Riesgos de Proceso/Proyecto /Producto **(Zona Baja)**	Oficina de Control Interno	**1.** Informar al líder del proceso sobre el hecho. **2.** Orientar las acciones a seguir al líder del proceso

Estrategias para combatir el riesgo (tratamiento)

Decisión que se toma frente a un determinado nivel de riesgo. Se analiza frente al Riesgo Residual.

- ✓ **Reducir:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación de este.
- ✓ **Transferir:** Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
- ✓ **Aceptar:** Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.
- ✓ **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo se implementan controles que mitiguen el nivel de riesgo.
- ✓ **Evitar:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

Cuando la decisión es **REDUCIR**, se requiere definir un **Plan de Acción**, el cual es una herramienta de planificación empleada para la gestión y control de tareas o proyectos. (No necesariamente es un control adicional. Se requiere establecer:

- ✓ Responsable
- ✓ Fecha de implementación
- ✓ Fecha de seguimiento

Nivel de Aceptación:

Una vez aplicado la tabla de probabilidad e impacto para cada riesgo se procede según su ubicación así:

Tipo de Riesgo	Zona de Riesgo	Tratamiento del Riesgo
Riesgos de Proceso, Producto y Proyecto	Baja	Se **ACEPTA** el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado; pueden existir escenarios de riesgos a los que no les pueden aplicar controles, por lo tanto, se acepta el riesgo. En ambos escenarios se debe realizar un seguimiento continuo del riesgo.
	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se hace seguimiento bimestral.
	Alta y Extrema	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan **EVITAR** la materialización del riesgo. Se monitorea mensualmente. **TRANSFERIR O COMPARTIR** una parte del riesgo para reducir la probabilidad o el impacto de este. Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.
	Baja	Ningún riesgo de corrupción podrá ser aceptado. Periodicidad **MENSUAL** de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de estos.

	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. Periodicidad mensual de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de estos.
Riesgos de Corrupción	Alta y Extrema	Se adoptan medidas para: **REDUCIR** la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. **EVITAR** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. **TRANSFERIR O COMPARTIR** una parte del riesgo para reducir la probabilidad o el impacto de este. Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos. (validar) está mal

Artículo 4° Monitoreo. El monitoreo debe estar a cargo de los responsables de los procesos, su finalidad principal es la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo.
El monitoreo debe asegurar que las acciones se están llevando a cabo y avaluar la eficiencia en su implementación, adelantando las revisiones sobre la marcha, para evidenciar todas aquellas situaciones o factores que puedan estar influyendo en la aplicación de las acciones preventivas.

En riesgos de corrupción el monitoreo también lo adelanta la oficina de planeación. La Oficina de Control Interno de Gestión realizará seguimiento tres (3) veces al año: el 1er seguimiento con corte al 30 de abril; el 2° seguimiento con corte al 31 de agosto y el 3er seguimiento con corte a 31 de diciembre. La publicación del informe de la Oficina de Control Interno se publicará dentro de los 10 días siguientes a dichas fechas, es decir para el 1er seguimiento dentro de los 10 días siguientes al 30 de abril. El 2° seguimiento dentro de los 10 días siguientes al 31 de agosto y el 3er ° seguimiento dentro de los 10 días siguientes al 31 de diciembre.

Artículo 5° Criterios Orientadores. Teniendo en cuenta que el adecuado manejo de los riesgos favorece el fortalecimiento del desarrollo institucional de la Gobernación Departamental, con el fin de asegurar dicho manejo es importante que los responsables del proceso, a través de las herramientas tecnológicas que sean implementadas, establezcan el entorno de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos, teniendo en cuenta las siguientes etapas o elementos establecidos en el Modelo Integrado de Planeación y Gestión - MIPG:

- Establecimiento del contexto: es la base para la identificación de los riesgos en los procesos y actividades. El análisis se realiza a partir del conocimiento de situaciones del entorno interno y externo de la entidad, tanto de carácter social, económico, cultural, ambiental, de orden público, político, legal y/o cambios tecnológicos, infraestructura, personal, entre otros; se alimenta también con el análisis de la situación actual de la entidad, basado en los resultados de los componentes de ambiente de control, estructura organizacional, modelo de operación, cumplimiento de los planes y programas, sistemas de información, procesos y procedimientos y los recursos económicos, entre otros.
- Identificación del Evento de Riesgo: el proceso de la identificación de riesgo debe ser permanente e interactivo basado en el resultado del análisis del contexto estratégico, en el proceso de planeación y debe partir de la claridad de los objetivos estratégicos de la entidad para la obtención de resultados.

  El modelo Estándar de Control Interno lo define como: Elemento de control que posibilita conocer los eventos potenciales, estén o no bajo en control de la Entidad Pública, que ponen en riesgo el logro de su Misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia.

La identificación de los riesgos se realiza a nivel del componente de direccionamiento estratégico, identificando los factores internos o externos a la entidad, que pueden ocasionar riesgos que afecten el logro de los objetivos. Es la base del análisis de riesgos que permite avanzar hacia una adecuada implementación de políticas que conduzcan a su control.

Se debe realizar determinando las causas, con base en los factores internos y/o externos que pueden afectar el equilibrio financiero del contrato.

Para los riesgos de activos de información se deben identificar aquellos eventos relacionados con la perdida de confidencialidad, integridad y de disponibilidad del activo de información.

- Análisis de Riesgo: el análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. El análisis del riesgo dependerá de la información obtenida, de la identificación de riesgo y de la disponibilidad de datos históricos y aportes de los servicios de la entidad.

  Para el análisis de los riesgos de los activos de información se debe identificar las causas que los generan por factores, circunstancias y/o agentes de vulnerabilidad y amenaza a que puede estar expuesta la información.

  Para el análisis de riesgos de la contratación estatal se cuantificará los riesgos previsibles que puedan afectar el equilibrio financiero mediante la estandarización de una metodología cuantitativa y/o semicuantitativo.

- Valoración del riesgo: La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados en el Elemento de Control, denominado "controles" del Subsistema de Control de Gestión, con el objetivo de establecer prioridades para su manejo y fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomas decisiones.

  Para realizar la valoración de los controles existentes es necesario recordar que estos se clasifican en:

  - **Controles Preventivos:** Están diseñado para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.
  - **Controles Detectives:** Controles que están diseñado para identificar un evento o resultado no previsto después de que se haya producido. Busca detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.
  - **Correctivo: (Después)** Acción que se ejecutan después de que se materializa el riesgo y en la mayoría de las ocasiones permiten reducir el impacto de dicho riesgo.

- Tratamiento de los riesgos: Para la consolidación de la política de administración de riesgos, se deben tener en cuenta todas las etapas anteriormente desarrolladas en el ejercicio de la administración del riesgo.

  Las acciones para tratar y manejar los riesgos basados en la valoración de estos permiten tomar decisiones adecuadas y fijar los lineamientos de la Administración del Riesgo, a su vez transmite la posición de la Gobernación Departamental y establecen las guías de acción necesarias a todos los servidores de la entidad, encaminadas a evitar, reducir, compartir o transferir, o finalmente asumir el riesgo.

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: implementación de acciones, definición de estándares, optimización de procesos y procedimientos y cambios físicos, entre otros. La selección de acciones debe considerar la viabilidad ambiental, jurídica, técnica, institucional, financiera y económica.

Para la ejecución de las acciones se debe identificar los responsables de llevarlas a cabo y definir el cronograma e indicadores que permitan verificar el cumplimiento, para tomar medidas preventivas y/o correctivas sea necesario.

Parágrafo. Para el tratamiento de los riesgos previsibles de la contratación de la Gobernación Departamental, se realizará desde el momento de elaborar los presupuestos y modelos financieros contenidos en los estudios previos que se adelantan en la etapa de planeación de la contratación. En la ejecución se debe monitorear los riesgos e implementar controles y acciones sobre los factores, buscando reducir el impacto económico de los riesgos identificados.

Artículo 6° Actualización. Los mapas de riesgo de cada uno de los procesos deberán ser actualizados anualmente y serán reportados a la Oficina Asesora de Control Interno, con el fin de ser presentados al comité institucional de coordinación de control interno. En ese sentido, los controles establecidos se revisarán y se ajustaran si es necesario, para adaptarlos a los cambios, situaciones o circunstancias por las que pueda atravesar la Entidad.

De manera semestral se deben realizar nuevas evaluaciones de probabilidad e impacto a través del aplicativo, teniendo en cuenta que los riesgos nunca dejan de representar una amenaza para la organización.

De acuerdo con los resultados, se deben actualizar o modificar las acciones de mitigación consignando las nuevas acciones y justificaciones en el plan de mitigación.

COMUNIQUESE, PUBLIQUESE Y CUMPLASE

21 SEP 2021

Angelica Hernandez

NIDIA ANGELICA HERNANDEZ
SECRETARIA DE PLANEACIÓN

Proyectó: htavera
Revisó: Ahernandez
Archivó: Abrackman