Enlace a Legislación Relacionada

GUÍA ESPECIALIZADA PARA LA EVALUACIÓN DE RIESGOS EN EL SECTOR PÚBLICO

RESOLUCIÓN N°. DGIDCA/DIDI/ODI/GUIA - N°. 7-2022, aprobada el 18 de agosto de 2022

Publicada en La Gaceta, Diario Oficial N°. 170 del 09 de septiembre de 2022

Los suscritos miembros del Consejo Superior de la Contraloría General de la República,

CONSIDERANDO:

I

Que la Constitución Política de la República de Nicaragua en su artículo 154 dispone que la Contraloría General de la República es el Organismo Rector del Sistema de Control de la Administración Pública y Fiscalización de los Bienes y Recursos del Estado; el artículo 155, numeral 1) faculta a la Contraloría General de la República a establecer el sistema de control que de manera preventiva asegure el uso debido de los fondos gubernamentales.

II

Que la Ley N°. 681, Ley Orgánica de la Contraloría General de la República y del Sistema de Control de la Administración Pública y Fiscalización de los Bienes y Recursos del Estado, en el artículo 9, denominado Atribuciones y Funciones, Numeral 2) establece: Dictar políticas, normas, procedimientos y demás regulaciones para: a) El funcionamiento del Control Interno.

III

Que la precitada Ley en el Título III, Sistema de Control de la Administración Pública y Fiscalización de los Bienes y Recursos del Estado, establece:

Capítulo I, Disposiciones Fundamentales.

Artículo 30 Marco Normativo General. Para regular el funcionamiento del Sistema de Control y Fiscalización, la Contraloría General de la República, expedirá: Numeral 5. Políticas, normativas, procedimientos, reglamentos, regulaciones, manuales generales

y especializados, guías metodológicas, instructivos y demás disposiciones necesarias para la aplicación del Sistemas de Control y Fiscalización y la determinación de responsabilidades.

Artículo 32 Componentes del Sistema de Control y Fiscalización. La ejecución del Sistema de Control de la Administración Pública y Fiscalización de los Bienes y Recursos del Estado, se realizará por medio de: Numeral 1. El Control Interno institucional, que es de responsabilidad administrativa de cada una de las instituciones de la Administración Pública.

Capítulo II, Del Control Interno Institucional, en los artículos 33 al 35, establece el concepto de Control Interno y su estructura, entre las cuales se establece la Evaluación de Riesgos y las formas de ejecución del Control Interno; también señala que el Control Interno es un proceso diseñado y ejecutado por la administración y otro personal de la entidad para proporcionar seguridad razonable con miras a la consecución de los siguientes objetivos:

1. Administración eficaz, eficiente, y transparente de los recursos del Estado;
2. Confiabilidad de la rendición de cuentas; y
3. Cumplimiento de las leyes y regulaciones aplicables.

Título VI Deberes y Atribuciones Generales, Capítulo Único, artículos 102 al 105, establecen que las Entidades y Organismo, las Máximas Autoridades y Titulares, los Directores o Jefes de Unidades Administrativas y servidores, tienen la responsabilidad del cumplimiento de los fines y objetivos institucionales de conformidad con el ordenamiento jurídico; asegurar la implantación, funcionamiento y actualización de los sistemas de administración y control interno; cumplir y hacer cumplir las disposiciones constitucionales, legales y reglamentarias, normas y demás disposiciones expedidas por la Contraloría General de la República. Los servidores deben cumplir los deberes, atribuciones y obligaciones de su cargo con transparencia, honradez y ética profesional y aplicar el Control Interno en las actividades a su cargo.

IV

Las Normas Técnicas de Control Interno (NTCI), infieren:

Capítulo II. Aspectos Técnicos de las NTCI.

2.3 Estructura del Control Interno, 2.4.2 Evaluación de Riesgos. Se centra en identificar y analizar los riesgos considerando su criticidad y tolerancia para la consecución de los objetivos de la Entidad, de tal forma, que se disponga de una base para dar respuesta a los mismos, a través de una adecuada administración.

2.5 Normas Específicas, numeral 2.5.2 Normas Específicas de Evaluación de Riesgos. Las instituciones deben de prever, conocer y abordar los riesgos con los que se

enfrentan, para establecer mecanismos que los identifiquen, analicen y disminuyan. Este proceso deberá ser dinámico e interactivo y que sirva de base para determinar cómo se gestionarán los riesgos en la Entidad.

Cada Entidad enfrenta una variedad de riesgos derivados de fuentes externas e internas, los cuales deben formar parte de la evaluación. Se entenderá por riesgo toda causa probable que interrumpa o impida la consecución de los objetivos de la Entidad.

Los principios que representan los conceptos fundamentales de la Evaluación de Riesgos, contienen los puntos de enfoque que detallan las características de los mismos, y servirán para determinar la efectividad del Control Interno, los cuales son:

Principio 6: Las Entidades definen objetivos con la suficiente claridad para permitir la identificación y evaluación de riesgos relacionados.

Principio 7: La Entidad identifica riesgos para el logro de sus objetivos y los analiza como base para determinar cómo deben ser administrados.

Principio 8: La Entidad considera la posibilidad de irregularidades en la evaluación de riesgos para el logro de los objetivos.

Principio 9: La Entidad identifica y evalúa los cambios que podrían afectar significativamente el sistema de control interno.

V

Que la Guías Especializadas para la Implementación del Sistema del Control Interno en las Instituciones Gubernamentales y Municipios de Nicaragua, en el capítulo V, Desarrollo de la Guía, 1. Breve descripción del Control Interno, 1.3 Componentes, Principios y Puntos de Enfoque, establece que la Evaluación de Riesgos provee las bases para identificar, analizar, calificar los riesgos (de fuentes internas o externas) que pueden impedir el cumplimiento de los objetivos institucionales y dar las respuestas apropiadas que mitiguen su impacto en caso de materialización.

Los principios relativos a las Actividades de Control, establecen entre otros que la Entidad selecciona y desarrolla actividades de control que contribuyen en la mitigación de riesgos al logro de los objetivos, a un nivel aceptable.

VI

Que las Entidades y Organismos de la Administración Pública, requieren de una herramienta que les proporcione la capacidad y competencia para el establecimiento e implementación de la gestión de riesgos como parte de la cultura organizacional, en la identificación, análisis, evaluación, tratamiento, comunicación y monitoreo de los riesgos, con la finalidad de gestionar una política de riesgos eficaz y eficiente que

asegure el cumplimiento de los objetivos y la misión de las Entidades y Organismos.

POR LO EXPUESTO:

El Consejo Superior de la Contraloría General de la República, en uso de las facultades conferidas en la Constitución Política de la República de Nicaragua y la Ley N°. 681, Ley Orgánica de la Contraloría General de la República y del Sistema de Control de la Administración Pública y Fiscalización de los Bienes y Recursos del Estado, publicada en La Gaceta, Diario Oficial, número 113 del 18 de junio del 2009, en sesión ordinaria número Un Mil Doscientos Noventa y Cinco (1295) a las nueve y treinta minutos de la mañana del día jueves dieciocho de agosto del año dos mil veintidós, aprobó por unanimidad de votos, dictar la siguiente actualización de la Guía denominada:

"Guía Especializada para la Evaluación de Riesgos en el Sector Público" (Actualización)

Comuníquese y publíquese. Dado en la ciudad de Managua, a los dieciocho días del mes de agosto del año dos mil veintidós.

(f) Dra. María José Mejía García, Presidenta del Consejo Superior, (f) **Dr. Vicente Chávez Fajardo,** Vicepresidente del Consejo Superior, (f) **Lic. Marisol Castillo Bellido**, Miembro Propietaria del Consejo Superior, (f) **Lic. María Dolores Alemán Cardenal,** Miembro Propietaria del Consejo Superior.

I. INTRODUCCIÓN

En la actualidad, las Entidades y Organismos de la Administración Pública, enfrentan diferentes tipos de riesgos procedentes de fuentes internas y externas relacionados con la administración de los bienes y recursos del Estado, por lo que deben contar con un sistema de control interno eficaz para lograr el cumplimiento de los objetivos institucionales. Un proceso de gestión de riesgos bien estructurado, consistente y coordinado es imprescindible para alcanzar este cometido.

Por esta razón, las Entidades u Organismos de la Administración Pública deben realizar acciones orientadas al fortalecimiento de una cultura de administración de riesgos a nivel institucional, para crear conciencia sobre los beneficios de su aplicación y de los efectos que pueden derivarse si no se los considera. Por tanto, es responsabilidad de las máximas autoridades de las Entidades y Organismos de la Administración Pública, la adopción de medidas para asegurar la gestión efectiva de los riesgos, especialmente aquellos de mayor importancia e impacto, para dotar a la comunidad de servicios públicos de calidad de forma oportuna.

En la administración moderna, en materia de riesgos se han emitido una serie de modelos, marcos, herramientas, técnicas que podrían ser utilizados por las Entidades y

Organismos, sin embargo la Contraloría General de la República de Nicaragua, con la finalidad de unificar criterios, ha considerado necesario desarrollar una metodología que se adecúe a las características organizacionales propias del sector gubernamental, como un esfuerzo inicial que permita establecer las bases de una implementación progresiva de modelos integrales en la gestión de riesgos.

La metodología presentada considera los lineamientos y herramientas que el Organismo de Control ha emitido en los temas de control interno, específicamente aquellos relacionados con la administración de riesgos.

La Guía Especializada para la Evaluación de Riesgos en el Sector Público describe entre otros aspectos el objetivo general, objetivos específicos, alcance, base legal y regulatoria, marco conceptual, organización y responsabilidades para la implementación y funcionamiento del proceso de administración de riesgos, metodología de administración de riesgos que incluye el desarrollo de las fases del proceso de gestión de riesgos, con sus respectivos anexos, formatos e instructivo para su utilización, así como ejemplos prácticos para facilitar su comprensión y aplicación.

Cabe señalar que esta Guía apunta a fortalecer el Sistema de Control Interno, mediante la generación de una visión sistémica sobre la administración y autoevaluación de riesgos; asimismo, a un direccionamiento estratégico que establezca una orientación de la gestión, proporcionando bases para el desempeño adecuado de las actividades de control.

Finalmente, esta Guía tiene como propósito dotar a las Entidades y Organismos de la Administración Pública un instrumento técnico para el manejo adecuado de los riesgos, que sea utilizado en toda la organización y que contribuya en la toma de decisiones para el uso adecuado de los bienes y recursos estatales en beneficio de la sociedad.

II. OBJETIVO GENERAL

Proporcionar a las Entidades y Organismos de la Administración Pública de una herramienta útil con los lineamientos para el proceso dinámico de administración de riesgos, que incluye el establecimiento del contexto, la identificación, análisis, evaluación, tratamiento, comunicación y monitoreo de los riesgos, con la finalidad de asegurar de forma razonable que se cumplan los objetivos institucionales en términos de eficiencia, eficacia y economía en un marco de transparencia y rendición de cuentas.

III. OBJETIVOS ESPECÍFICOS

- Contribuir a la administración en la identificación y análisis de los riesgos que afecten el cumplimiento de los objetivos institucionales, relativos a los procesos críticos de las Entidades y Organismos de la Administración Pública.

- Dotar a la máxima autoridad, titulares, directivos y servidores de las Entidades y Organismos de la Administración Pública y auditores internos de un instrumento, para la administración y evaluación de riesgos para proteger los recursos gubernamentales.

- Orientar a que cada Entidad y Organismo y sus servidores incluyan en sus procesos y procedimientos, acciones de prevención y administración de riesgos para el cumplimiento de su misión, objetivos y funciones institucionales.

IV. ALCANCE

La presente Guía Especializada para la Evaluación de Riesgos en el Sector Público, proporciona directrices para establecer y mantener un marco técnico para la administración general de riesgos, que permita a los servidores públicos de las Entidades y Organismos de la Administración Pública en su conjunto, gestionar los riesgos de manera eficaz y eficiente para el logro de los objetivos institucionales; fortaleciendo su desempeño y promoviendo una constante evaluación e implementación de mejoras continuas en los procesos sustantivos y de apoyo.

V. BASE LEGAL Y REGULATORÍA

- Constitución Política de la República de Nicaragua.

- Ley N°. 681, Ley Orgánica de la Contraloría General de la República y del Sistema de Control de la Administración Pública y Fiscalización de los Bienes y Recursos del Estado, publicada en la Gaceta, Diario Oficial N°.113 del 18 de junio del 2009.

- Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI): GOV 9100 Guía para las normas de control interno del sector público; GOV 9110 Directrices referentes a los informes sobre la eficacia de los controles internos: Experiencias de las EFS en la implantación y la evaluación de los controles internos; y GOV 9130 Guía para las Normas de Control Interno del sector público-información adicional sobre la Administración de Riesgos de la Entidad.

- Informe COSO (Committe of Sponsoring Organizations of the Treadway Commission) 2013.

- Normas Técnicas de Control Interno (NTCI), emitidas por la Contraloría General de la República de Nicaragua, publicada en la Gaceta, Diario Oficial N°.67 del 14 de abril del año 2015.

- Guía Especializada para la Implementación del Sistema de Control Interno en las Instituciones Gubernamentales de Nicaragua, emitida por la Contraloría General de la República de Nicaragua, publicada en la Gaceta, Diario Oficial N°.07 del 14 de enero del año 2020.

-Guía Especializada para la Implementación del Sistema de Control Interno en los Municipios de Nicaragua, emitida por la Contraloría General de la República de Nicaragua, publicada en la Gaceta, Diario Oficial N°. 11 del 20 de enero del año 2020.

VI. DEFINICIONES DE TÉRMINOS

En la presente Guía se destacan las siguientes acepciones:

Aceptación del riesgo. Una decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

Administración de riesgos. Es el término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de forma que permita a las organizaciones asegurar el logro de sus objetivos y metas de una manera razonable.

Análisis del riesgo. Proceso sistemático para entender la naturaleza del riesgo y determinar el nivel del riesgo. El análisis de riesgo proporciona las bases para la valoración del riesgo. El análisis debe considerar el rango de consecuencias potenciales y cuán probable es que los riesgos puedan ocurrir. El Impacto, la probabilidad e importancia se combinan para producir un nivel estimado de riesgo según la organización.

Análisis del costo beneficio. Herramienta de administración de riesgos usada para tomar decisiones sobre las técnicas propuestas para la administración de riesgos, en la cual se valoran y comparan los costos financieros y económicos de implementar la medida, contra los beneficios generados por la misma. Una medida de administración de riesgos será aceptada siempre que el beneficio valorado supere el costo.

Apetito de riesgo. Es la cantidad de riesgo a nivel global que la entidad u organismo está dispuesta a aceptar en su búsqueda de valor. Este puede ser establecido en relación a la organización como un todo, para diferentes grupos de *riesgo o en un nivel de riesgo individual.*

Control de riesgos. Proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo el riesgo e incrementar la probabilidad de lograr los objetivos y metas institucionales. La Entidad u Organismo implementará las actividades necesarias para proporcionar seguridad razonable de que se alcanzarán los objetivos y metas.

Consecuencia. Resultado o impacto de un evento, expresado cualitativamente o cuantitativamente.

Evaluación del control. Revisión sistemática de los controles para garantizar que son eficaces y adecuados en la administración del riesgo.

Evaluación de riesgos. El proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel de riesgo respecto de estándares predeterminados, niveles de riesgos, objetivos u otros criterios.

Evento. Ocurrencia de un conjunto particular de circunstancias. Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo particular. Un incidente o acontecimiento derivado de fuentes internas o externas a la Entidad u Organismo, que afecta a la consecución de los objetivos.

Evitar un riesgo. Una decisión informada de no verse involucrado en una situación de riesgo.

Eficiencia. El logro de objetivos y metas programadas utilizando la menor cantidad de recursos.

Eficacia. Cumplir con los objetivos y metas planteadas en lugar, tiempo, calidad y cantidad previstos.

Economía. Los términos y condiciones bajo los cuales se adquieren recursos, en cantidad, calidad apropiada y al menor costo posible para realizar una actividad determinada.

Frecuencia. Medición del número de ocurrencias por unidad de tiempo.

Identificación de riesgos. El proceso de determinar qué puede suceder, por qué y cómo.

Impacto. El resultado o efecto de un evento. Pueden existir una gama de posibles impactos asociados a un evento. El impacto de un evento puede ser positivo o negativo sobre los objetivos relacionados de la Entidad y Organismo.

Monitoreo. Verificar, supervisar o medir regularmente el progreso de una actividad, acción o sistema para identificar los cambios en el nivel de desempeño requerido.

Política. Directrices de la administración de lo que debe hacerse para efectuar los controles. Una política sirve como base para la implantación de procedimientos.

Posibilidad. Se usa como descripción general de la probabilidad o la frecuencia. Ejemplo: nunca, alguna vez o siempre.

Probabilidad. Medida o descripción de la posibilidad de ocurrencia de un evento negativo.

La posibilidad de que un evento dado ocurra. Los términos a veces adquieren

connotaciones más específicas y “probabilidad” tanto puede indicar dicha posibilidad en términos cualitativos como alto, medio, bajo derivados de otras escalas de juicio, o bien indicarla mediante una medida cualitativa, como porcentaje, frecuencia de ocurrencia u otra métrica numérica.

Proceso de gestión. Serie de acciones tomadas por la dirección para conducir una entidad. La administración de riesgos institucionales es una parte del proceso de gestión y está integrada en él.

Reducción del riesgo. Acciones que se toman para reducir la posibilidad y consecuencias asociadas a un riesgo. Una aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de ocurrencia, sus consecuencias, o ambas.

Riesgo. La probabilidad que ocurra un acontecimiento (externo o interno) que provoque un impacto negativo en el logro de los objetivos y metas de la Entidad u Organismo. Se mide en términos de probabilidad e impacto.

Riesgo aceptado. La cuantía más amplia del riesgo que una Entidad u Organismo está dispuesta a asumir para realizar su misión o visión.

Riesgo Inherente. El riesgo al que se somete una entidad en ausencia de acciones de la dirección para alterar o reducir su probabilidad de ocurrencia e impacto.

Riesgo residual. Riesgo remanente después de la implementación del tratamiento del riesgo. El riesgo remanente después de que la dirección haya llevado a cabo una acción para modificar la probabilidad o impacto de un riesgo.

Transferir riesgos. Cambiar la responsabilidad a una tercera parte mediante legislación, contrato, seguros u otros medios. También se puede referir a cambiar un riesgo físico o parte del mismo a otro sitio.

Tratamiento de riesgos. Selección o implementación de opciones apropiadas para tratar el riesgo.

Tolerancia al riesgo. Es el nivel aceptable de desviación relativo a la consecución de objetivos. Pueden ser medidos a través de los objetivos de desempeño. Frecuentemente las metas de rendimiento se miden mejor si es posible, con las mismas unidades que los objetivos correspondientes. El funcionamiento dentro de la tolerancia del riesgo, proporciona mayor aseguramiento para la gerencia de que la entidad u organismo permanezca dentro de su riesgo aceptado y logre sus objetivos.

Valoración del riesgo. Proceso total de identificación, análisis y evaluación del riesgo para priorizarlos luego de la confrontación con los controles existentes, que permite establecer los que pueden causar mayor impacto a la Entidad u Organismo.

Fuente: http://www.leybook.com/doc/28679

VII. MARCO CONCEPTUAL

La administración de riesgos parte de la planificación estratégica, la misión, la visión, objetivos estratégicos y valores institucionales, así como de la identificación de eventos potenciales que, de ocurrir, podrían afectar a la Entidad u Organismo en la consecución de sus objetivos fundamentales. Cuando los eventos pueden afectar negativamente en la implantación de la estrategia y objetivos representan ***riesgos,*** y exigen la evaluación y respuesta por parte de la dirección, de lo contrario, si tienen un impacto positivo representan ***oportunidades*** a ser reconducidas para implantar la estrategia y lograr los objetivos con éxito.

Cuando la dirección identifica los eventos negativos y positivos, contempla una serie de factores internos y externos que pueden dar lugar a riesgos y oportunidades, que requieren ser evaluados y tomar acciones de respuesta con la finalidad de evitar o anular, reducir, compartir y aceptar los mismos a fin de garantizar la gestión institucional y el logro de los objetivos.

El riesgo es un concepto fundamental, se afirma que no existe una actividad de la vida que no incluya la palabra riesgo, por esa razón el ser humano ha buscado siempre protegerse de las contingencias, investigando maneras de evitar o anular, reducir y compartir los riesgos a través de acciones preventivas.

Para efectos de la Guía Especializada, se considera ***riesgo*** a toda probabilidad de un evento que pueda entorpecer o impedir el normal desarrollo de las actividades de la Entidad u Organismo de la administración pública en su conjunto y afecte el logro de sus objetivos.

El riesgo está presente en todas las operaciones de cualquier Entidad u Organismo de la Administración Pública y se materializa mediante eventos adversos que detonan en pérdidas directas o indirectas, costos por daños de imagen, ineficiencia de procesos internos, deficiencia en la administración de personal, y anomalías en los sistemas automatizados, entre otras consecuencias inesperadas.[1]

1 Guía de Autoevaluación de Riesgos en el Sector Público-Auditoría de Federación Superior (ASF)

La evaluación de riesgos permite a una Entidad u Organismo considerar la amplitud con que los eventos potenciales impactan en la consecución de objetivos. La dirección analiza y evalúa estos acontecimientos desde una doble perspectiva - probabilidad e impacto - y normalmente usa una combinación de métodos cualitativos y cuantitativos. Los impactos positivos y negativos de los eventos potenciales deben examinarse, individualmente o por categoría, en toda la entidad. Los riesgos se evalúan con un doble enfoque: riesgo inherente y riesgo residual.[2]

2 INTOSAI GOV 9130- Guía para las normas de control interno del sector público. Información adicional

sobre la administración de riesgos de la entidad.

No existen dos Entidades u Organismos que apliquen o debieran aplicar la administración de riesgos del mismo modo. Sus capacidades y sus necesidades de administración de riesgos difieren sustancialmente según su dimensión, actividad, filosofía y cultura de la dirección. Así, aunque todas las entidades deberían tener cada componente operando efectivamente, la aplicación de la administración de riesgos en una entidad, incluyendo las herramientas y técnicas aplicadas, así como la asignación de roles y responsabilidades, a menudo no tendrá el mismo aspecto que la empleada en otras entidades.[3]

3 Resumen de los componentes de la Administración de Riesgos Corporativos, Marco Integrado, Diciembre 2005

Las Normas Técnicas de Control Interno, publicadas en la Gaceta, Diario Oficial NO. 67 del 14 de abril del año 2015, establecen en las Normas Específicas de Evaluación de Riesgos:

-Principio 6: Las Entidades definen objetivos con la suficiente claridad para permitir la identificación y evaluación de riesgos relacionados.

La Máxima autoridad define tres categorías de objetivos: Operacionales, de Información y de Cumplimiento, consistentes con su misión, con la suficiente claridad para permitir la identificación y evaluación de riesgos. La administración deberá prever, conocer y abordar los riesgos con los que se podrán enfrentar los objetivos de la Entidad u Organismo.

-Principio 7: La Entidad identifica riesgos para el logro de sus objetivos y los analiza como base para determinar cómo deben ser administrados.

La Máxima Autoridad deberá velar porque los riesgos estén siendo identificados mediante un mapeo de riesgos, que incluya la especificación de sus procesos claves. La Máxima Autoridad y la Administración deberán identificar los factores tanto internos como externos, que influyen en la ocurrencia de riesgos tales como: severidad, velocidad y persistencia del riesgo, la probabilidad de pérdida de activos y el impacto relacionado sobre las actividades operativas, de reporte y cumplimiento. La Administración deberá efectuar el proceso de identificación de riesgos de forma integral y completa en toda la Entidad; analizando la probabilidad de ocurrencia, el impacto que causaría y la importancia del riesgo, para definir cómo serán manejados: aceptados, anulados, reducidos o compartidos.

-Principio 8: La Entidad considera la posibilidad de irregularidades en la evaluación de riesgos para el logro de los objetivos.

La Administración debe considerar los posibles actos irregulares, ya sea del personal

de la Entidad o de los Proveedores de servicios externos, que afectan directamente el cumplimiento de los objetivos.

-Principio 9: La Entidad identifica y evalúa los cambios que podrían afectar significativamente al Sistema de Control Interno.

La Administración debe considerar dentro de la evaluación de riesgos el establecimiento de controles para identificar y comunicar los cambios en el contexto, modelo de la Entidad u Organismo y en el liderazgo, que podrían afectar sus objetivos.

La diversidad de Entidades y Organismos que conforman la Administración Pública, difieren en su tamaño, complejidad, sector, cultura, estilo de administración y otros atributos propios de cada una de ellas, lo que puede afectar el modo de implementar el Control Interno de la manera más efectiva y eficiente posible, por esta razón en esta Guía se introducen determinados puntos en común que podrían aplicarse a todas las Entidades y Organismos.

La Guía plantea un modelo general de matriz para la calificación de riesgos, que aplicada permitirá identificar las áreas de gestión críticas o con riesgos calificados como altos, moderados o bajos. Su aplicación dependerá de las características y particularidades especiales de cada una de las Entidades y Organismos de la Administración Pública.

VIII. ORGANIZACIÓN Y RESPONSABILIDADES PARA LA IMPLEMENTACIÓN Y FUNCIONAMIENTO DEL PROCESO DE ADMINISTRACIÓN DE RIESGOS

Responsables y Roles

Es importante señalar que cada una de las fases del Proceso de Gestión de Riesgos es en primer lugar responsabilidad de la máxima autoridad de la Entidad u Organismo, de la administración y de los servidores públicos responsables de cada proceso.

Para lograr la implementación del proceso de administración de riesgos, se deberá establecer los **responsables del proceso y sus roles,** definir, documentar y aprobar la responsabilidad, autoridad e interrelaciones del personal que debe realizar las acciones relacionadas con esta materia y que se resumen a continuación:
- Iniciar acciones para prevenir o reducir los efectos de los riesgos.

- Controlar el tratamiento de los riesgos.

- Identificar y registrar cualquier problema relacionado con la gestión de los riesgos.

- Iniciar, recomendar o proveer soluciones a través de estrategias.

- Verificar a través del monitoreo la implementación de las soluciones contenidas en

las estrategias.[4]

4 Documento Técnico No. 70, versión 0.2 Implantación, mantención y actualización del proceso de gestión de riesgo en el sector público, del Consejo de Auditoria Interna General del Gobierno de Chile, Año 2016.

Gráficamente, la organización para la implementación y funcionamiento del proceso de administración de riesgos es el siguiente:

Los responsables y roles se detallan a continuación:

Máxima Autoridad:

Rol clave: Supervisor y Coordinador de decisión.
1. Estimular la cultura de la identificación y prevención de riesgos.
2. Aprobar la política de riesgos.
3. Brindar retroalimentación sobre la efectividad del Proceso de Gestión de Riesgos.
4. Definir los canales y espacios de comunicación de la política de riesgos institucional.
5. Nombrar el Comité de Administración de Riesgos conformado por Responsables de las áreas sustantivas, apoyo y staff, con el nivel de autoridad en la toma de decisiones.

Comité de Administración de Riesgos:

Rol clave: Supervisor y Asesor.

Será responsable de la revisión del diseño e implementación del Proceso de Gestión de Riesgos, proporcionando a la máxima autoridad reportes del avance en la implementación y la efectividad de las estrategias de mitigación.
1. Revisar y proponer ajustes al diseño e implementación del Proceso de Gestión de Riesgos y a las políticas de riesgo institucional, para autorización de la máxima autoridad.
2. Supervisar la implementación del Proceso de Gestión de Riesgos, la estrategia de tratamiento de riesgos y la efectividad.
3. Monitorear el perfil de riesgo o el nivel de tolerancia de la Entidad u Organismo.
4. Asegurar que los riesgos han sido considerados en planes de largo plazo.
5. Informar a la máxima autoridad sobre la planificación y avances del diseño e implementación del Proceso de Gestión de Riesgos.
6. Desarrollar planes de contingencias ante la presencia de riesgos y presentar a la máxima autoridad para su aprobación.
7. Revisar frecuentemente la exposición a las amenazas internas y externas.

Encargado de Riesgos (Área organizativa de Planificación o el área que determine la máxima autoridad):

Será responsable del proceso de diseño e implementación de la gestión de riesgos de la Entidad u Organismo en coordinación con los directivos responsables de cada área, así como del seguimiento continuo de la implementación de las actividades del riesgo.

Rol clave: Comprensión de Riesgos.

1. Formular el diseño e implementación del Proceso de Gestión de Riesgos y políticas de riesgo institucional, para revisión del Comité de Administración de Riesgos.

2. Dirigir, orientar y coordinar el diseño e implementación del Proceso de Gestión de Riesgos con los directivos responsables de cada área.

3. Dirigir el avance general de la implementación de las estrategias de tratamiento de riesgos.

4. Asegurar la ejecución de todas las fases previstas en el diseño del Proceso de Gestión de Riesgos.

5. Informar al Comité de Administración de Riesgos sobre la planificación y avances del diseño e implementación del Proceso de Gestión de Riesgos.

6. Consolidar las matrices de evaluación de riesgos y plan de tratamiento o mitigación de riesgos elaborados por las Unidades Organizativas en una matriz de riesgos y plan de mitigación institucional.

7. Definir prioridades del riesgo y el nivel de tolerancia en coordinación con los Responsables de las Unidades Organizativas.

8. Alinear la respuesta al riesgo a todas las estrategias de la organización y objetivos institucionales.

9. Efectuar el seguimiento y monitoreo a las actividades planteadas en el diseño e implementación del Proceso de Gestión de Riesgos.

10. Arbitrar y resolver conflictos.

11. Evaluar la efectividad del Proceso de administración de riesgos.

12. Dar seguimiento a los planes de contingencias.

Responsables de Riesgos de Unidades Organizativas (Directores o Responsables de áreas):

Rol clave: Operación y soporte.

Administrar y reportar riesgos a nivel del área de gestión al Encargado de Riesgos, designado para el diseño e implementación del Proceso de Gestión de Riesgos. Elaborar las matrices de riesgos e implementar el plan de tratamiento de riesgos.

1. Identificar, analizar y evaluar los riesgos en el área de gestión, elaborando las matrices de riesgos por unidad organizativa.

2. Alinear las prioridades de identificación de riesgos.

3. Calificar y medir el impacto, la probabilidad y la importancia de los riesgos.

4. Formular respuestas apropiadas al riesgo, mediante la elaboración del plan de tratamiento o mitigación de riesgos.

5. Determinar el nivel de tolerancia del riesgo de su unidad organizativa.

6. Efectuar propuestas de mejora continua de mediciones y procesos.

7. Monitorear el avance en su área en la implementación de las estrategias de tratamiento de los riesgos.

Es importante señalar que el Auditor Interno de la Entidad u Organismo no puede ser nombrado como responsable en estos temas, ya que se estaría afectando su objetividad e independencia al momento de auditar el funcionamiento y efectividad del Proceso de Gestión de Riesgos (actividad de aseguramiento). A continuación, se señala el rol de la Unidad de Auditoría Interna en un Proceso de Gestión de Riesgos, destacándose aquellas funciones que puede realizar y aquellas que no están permitidas.

Auditoría Interna [5]

5 Documento Técnico No. 70, versión 0.2 Implantación, mantención y actualización del proceso de gestión de riesgo en el sector público, del Consejo de Auditoría Interna General del Gobierno de Chile, Año 2016.

Rol de la Auditoría Interna: El rol fundamental de la Auditoría Interna en el Proceso de Gestión de Riesgos será proveer asesoría o apoyo al Comité de Administración de Riesgos sobre la efectividad de las actividades del Proceso de Gestión de Riesgos, para ayudar a asegurar que los riesgos claves del servicio público están siendo gestionados apropiadamente y que el sistema de control interno está siendo operado efectivamente.

El Auditor Interno debe proveer asesoría sobre riesgos, y no tomar decisiones sobre gestión del riesgo; debe tomar en cuenta si la actividad representa alguna amenaza sobre la independencia y objetividad al realizar su trabajo, y si podría mejorar el

Proceso de Gestión de Riesgo y el control interno en la organización.

1.1. Principales roles de Auditoría Interna recomendados en el Proceso de Gestión de Riesgo en las Entidades y Organismos de la Administración Pública:

1. Efectuar asesoría al Comité de Administración de Riesgos, sobre el Proceso de Gestión de Riesgos, para que los riesgos sean correctamente evaluados.

2. Evaluar el Proceso de Gestión de Riesgo.

3. Revisar el manejo y evaluación de los reportes de riesgos claves.

4. Evaluar la elaboración de informes sobre los riesgos claves.

5. Revisar la gestión de riesgos claves.

1.2 Roles de Auditoría Interna que deben realizarse con independencia y objetividad en el Proceso de Gestión de Riesgos en las Entidades y Organismos de la Administración Pública:

1. Brindar asesoría en la identificación y evaluación de riesgos.

2. Asesorar al Comité de Administración de Riesgos para responder a los riesgos.

3. Asesorar en el desarrollo de estrategias de gestión del riesgo en las áreas de gestión de la Entidad u Organismo.

A continuación, se describen algunos roles que la Auditoría Interna NO debe realizar en el Proceso de Gestión de Riesgos en las Entidades u Organismos del Estado:

1. Establecer el nivel de riesgo aceptado.

2. Imponer Procesos de Gestión de Riesgos.

3. Manejar el aseguramiento sobre los riesgos.

4. Tomar decisiones sobre las respuestas a los riesgos.

5. Implementar respuestas a los riesgos.

6. Tener roles de responsabilidad de la gestión de los riesgos.

IX. METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS

PROCESO DE GESTIÓN DE RIESGOS

La gestión de riesgos es un proceso estructurado, consistente y continúo implementado a través de toda la organización para identificar, analizar, evaluar, medir y reportar amenazas que afectan el poder alcanzar el logro de sus objetivos. Todos en la organización juegan un rol en el aseguramiento del éxito de la gestión de riesgos, pero la responsabilidad principal de la identificación y manejo de éstos recae sobre la máxima autoridad.[6]

6 COSO II - ERM

La definición anterior se complementa con los siguientes elementos:

• Es un proceso interactivo que contribuye a la mejora institucional a través del perfeccionamiento de los procesos.

• Es de aplicación a todos los niveles de la organización: estratégicos, tácticos y operacionales.

• Puede ser aplicada a proyectos específicos, para sustentar las decisiones o para administrar áreas de riesgo.

• Para cada fase del Proceso de Gestión de Riesgos deberían mantenerse registros adecuados, suficientes como para satisfacer a una auditoría externa o certificación independiente.

• No solo considera la identificación y tratamiento de riesgos, sino también las oportunidades que contribuyan al logro de los objetivos.

• La aplicación del marco teórico del Proceso de Gestión de Riesgos, debe adecuarse a la Entidad u Organismo de la Administración Pública.

La principal obligación de las Entidades y Organismos de la Administración pública es el cumplimiento de la misión y los objetivos planteados en su Ley o Decreto de creación, identificados en los planes estratégicos, operativos, programas, proyectos, actividades y tareas definidos con esa finalidad; sin embargo, la ejecución de esos programas y proyectos pueden verse afectados por la presencia de factores negativos internos o externos, que es necesario identificarlos, analizarlos, valorarlos y definir acciones para su mitigación.

Un manejo adecuado de los riesgos permite el desarrollo de la Entidad u Organismo, para ello es importante establecer el contexto en el que se desenvuelve la organización, así como la identificación, análisis, valoración y definición de las alternativas de actividades de tratamiento de los riesgos.

El Proceso de Gestión de Riesgos se sintetiza en el siguiente esquema: [7]

7. AS/NZS 4360:1999, Estándar Australiano, Administración de Riesgos

FASE 1: ESTABLECER EL CONTEXTO

En esta fase se analiza el contexto estratégico, organizacional y de gestión, en los cuales se basará y desarrollará el Proceso *de Gestión de Riesgos*.

El establecimiento del contexto estratégico significa analizar el entorno externo en el que funciona la Entidad u Organismo de la Administración Pública, considerando los aspectos financieros, operativos, competitivos, políticos, imagen, sociales, clientes, usuarios, culturales, legales, proveedores, tecnológicos, comunidad o sociedad en general.

El contexto organizacional o interno significa comprender la estructura interna, los recursos humanos, filosofía, valores institucionales, políticas, misión, metas, objetivos y estrategias para alcanzar los objetivos.

En esta etapa del proceso es importante que los responsables de la implementación del proceso de administración de riesgos conozcan el funcionamiento general de la Entidad u Organismo, así como las metas u objetivos estratégicos de la misma. Para lograr lo anterior se recomiendan que los servidores públicos revisen:

- Documentos como: el Plan Estratégico, Programa Sectorial y Plan Nacional de Lucha contra la Pobreza y para el Desarrollo Humano y otros documentos vinculantes al proceso, con el propósito de conocer la misión, visión, valores y directrices generales de la Entidad u Organismo en un marco general.

- La estructura orgánica de la Entidad u Organismo, así como las atribuciones en el ámbito de su competencia (Manual de Organización y Funciones).

- Planes operativos de las unidades organizativas.

- La alineación de las metas y objetivos particulares de cada unidad organizativa con las metas y objetivos estratégicos.[8]

8 Guía de Autoevaluación de Riesgos en el Sector Público-Auditoria Superior de la Federación (ASF).

Se ilustra con un ejemplo la vinculación existente entre los objetivos estratégicos, objetivos operativos y objetivos específicos de una organización. *Anexo N°.1.*

La mayoría de las Entidades y Organismos de la Administración Pública han definido su contexto estratégico y operativo, tienen identificada su misión y visión, así como los objetivos estratégicos, operativos y específicos en sus planes respectivos, han

establecido metas e indicadores; es decir, han identificado los elementos de su entorno interno y externo.

La administración de las Entidades u Organismos deben definir la tolerancia al riesgo para los objetivos definidos. Dicha tolerancia es el nivel aceptable de diferencia entre el cumplimiento cabal del objetivo y su grado real de cumplimiento. Las tolerancias al riesgo son inicialmente fijadas como parte del proceso de establecimiento de objetivos. La administración debe definir las tolerancias al riesgo en términos específicos y medibles de modo que sean claramente establecidas y puedan ser medidas. La tolerancia es usualmente medida con las mismas normas e indicadores de desempeño que los objetivos definidos y se debe evaluar si las tolerancias al riesgo permiten el diseño apropiado del control interno al considerar si son consistentes con los requerimientos y las expectativas de los objetivos definidos. Como en la definición de los objetivos, se debe considerar las tolerancias al riesgo en el contexto de las leyes, regulaciones y normas aplicables a la Entidad u Organismo.[9]

9 Marco integrado de control interno, Auditoría Superior de la Federación (ASF), Secretaría de la Función Pública (SFP), Estados Unidos Mexicanos, año 2014.
INSTOSAI GOV 9130 Guía para las Normas de Control Interno del Sector Público. Información adicional sobre la Administración de Riesgos de la Entidad.

El Apetito de Riesgo es una aprobación de alto nivel de aceptación de un riesgo en el logro de los objetivos principales.

La Tolerancia al Riesgo es el nivel aceptable de diferencia respecto al logro de los objetivos, así como la cantidad máxima de un riesgo que una institución puede soportar sin causar graves daños al logro de los propósitos de la entidad u organismo. A continuación, se muestran sus principales características:

• Es posible medir y contrastarla con los objetivos (en los mismos términos).

• Debe mantener coherencia con el apetito al riesgo (que nivel de riesgo está dispuesto aceptar).

• Establecer riesgos que la institución no está dispuesta aceptar (por ejemplo: en el cumplimiento del marco legal).

Actividades para Emprender la Gestión de Riesgos

Los elementos anteriores constituyen la base para emprender la *gestión* de riesgos en la Entidad u Organismo, de la siguiente forma:

Acciones

a) Compromiso: Para el éxito de la administración de riesgos, es indispensable en la

Entidad u Organismo la integración de la máxima autoridad, la definición de políticas, así como el establecimiento de una estructura interna integrada por: el Comité de Administración de Riesgos, Encargado de Riesgos (Área Organizativa de Planificación o el área que determine la máxima autoridad) y Responsables de Riesgos por Área de Gestión (Responsables de Unidades Organizativas), para promover una cultura de identificación y prevención de riesgos, así como definir políticas relacionadas con la administración de riesgos.

El Encargado de Riesgos (Área Organizativa de Planificación o el área que determine la máxima autoridad), deberá dirigir, coordinar y asesorar las acciones para desarrollar la gestión de riesgos, con el fin de contribuir a la consecución de las metas y objetivos establecidos en los planes.

b) Conformación del equipo: Es importante que las Entidades u Organismos cuenten con un equipo de servidores de las diferentes áreas de la organización, responsables de la implementación del proceso de administración de riesgos. Es recomendable que los integrantes de este equipo cuenten con conocimientos sobre la Entidad u Organismo y sobre control interno, administración de riesgos e integridad en el sector público, con el fin de que se facilite la identificación, análisis, evaluación, respuesta, supervisión y comunicación de los riesgos.-

c) Capacitación sobre la Guía: Una vez que la Entidades u Organismos cuenten con el equipo responsable que participará en el proceso de administración de riesgo, la Dirección General de Investigación, Desarrollo y Capacitación Aplicada (DGIDCA) a través de la División del Centro de Capacitación de la Contraloría General de la República, capacitará a sus integrantes en la aplicación del presente documento.

Política de Gestión de Riesgos

La política de riesgos deberá indicar claramente los objetivos y compromisos de la Entidad u Organismo en materia de la gestión de riesgos, lo que será coherente con la política de calidad de las actividades o servicios que tengan las Entidades u Organismos de la Administración Pública. La política de riesgos será publicada y comunicada a todos los niveles de dicha organización. Contendrá entre otros aspectos:

- Los enlaces entre los objetivos y las políticas de la organización y las políticas de gestión de riesgos.-

- Las obligaciones de rendir cuentas y las responsabilidades en materia de gestión de riesgos.

- La manera en que se tratan los intereses que entran en conflicto.

- El compromiso con el fin de tener disponibles los recursos necesarios para ayudar a

aquellos con la obligación de rendir cuentas y responsables por la gestión de riesgos.

- La manera en la que se mide e informa el desempeño de la gestión del riesgo.

- El compromiso para revisar y mejorar la política de gestión del riesgo y el marco del trabajo, periódicamente y como respuesta a un evento o a un cambio de circunstancias.[10]

10 Documento Técnico No. 70, versión 0.2 Implantación, mantención y actualización del proceso de gestión de riesgo en el sector público, del Consejo de Auditoría Interna General del Gobierno de Chile, Año 2016.

Etapas para la Implementación de Gestión de Riesgos

La organización debe definir un programa de implementación de gestión de riesgos, en función del tamaño y/o complejidad, filosofía, cultura y estructura de la organización identificando los requerimientos de recursos, con personal entrenado o capacitado para estas actividades.

En el ***Anexo N°.2***, se describen las etapas para la implementación del Proceso de Gestión o Administración de Riesgos.

Diccionario de Riesgos

Se considera necesario establecer un diccionario de riesgos para cada Entidad u Organismo, que contenga a nivel estratégico los riesgos a los que está expuesta la organización.

Con esta finalidad, todos los mandos medios necesitan considerar los eventos que pueden impactar sus áreas de actividad y ponerlos en conocimiento al Comité de Administración de Riesgos para que este a su vez informe a la máxima autoridad de la Entidad u Organismo con sus posibles soluciones. La máxima autoridad debe utilizar estas evaluaciones a través de todos los niveles y áreas de gestión para construir una evaluación general del portafolio de riesgos de la organización.

Para llevar a cabo los **análisis de contexto** (factores externos e internos de riesgos) es necesario que los responsables de las Unidades Organizativas utilicen herramientas como: entrevistas, cuestionarios y lluvia de ideas con los servidores públicos de diferentes niveles jerárquicos expertos en el funcionamiento de los procesos de la institución. También es importante llevar a cabo indagaciones con personas ajenas a la Entidad u Organismo, analizar los escenarios (supuestos de materialización de riesgos) y revisar de manera periódica factores económicos, tecnológicos, de regulación, entre otros, que puedan afectar el funcionamiento de la Entidad u Organismo.

En relación a la fuente u origen de los riesgos, existen dos tipologías:

1. Los riesgos de fuente externa que tienen origen en situaciones que no están bajo control de la Entidad u Organismo y del servicio que esta presta.

Los factores externos pueden ser:

- Económicos: Cambios económicos que pueden impactar en las condiciones financieras de la Entidad u Organismo.

- Ambiente Natural: Catástrofes naturales o causadas por el ser humano, o cambios climáticos que puedan generar cambios en las operaciones, reducción en la disponibilidad de insumos o recursos críticos para la operación, pérdida de sistemas de información resaltando la necesidad de planes de contingencia.

- Factores Regulatorios: Nuevas políticas, regulaciones y leyes que impliquen cambios en las estrategias operativas y de reporte de la Entidad u Organismo.

- Factores Sociales: Cambios en las necesidades y expectativas de los ciudadanos que puedan afectar el desarrollo de los productos o servicios que provee la Entidad u Organismo.

- Operaciones Extranjeras: Cambios en el gobierno o leyes de países extranjeros que afecten a la Entidad u Organismo.

- Factores Tecnológicos: Cambios tecnológicos que pueden afectar en la disponibilidad y uso de la información, costos de infraestructura y la demanda de los servicios basados en la tecnología.

2. Los riesgos de fuente interna que se originan en la propia organización o al interior de los procesos.

Los factores internos pueden ser:

- Infraestructura: Decisiones sobre el uso de recursos financieros que pueden afectar las operaciones y la disponibilidad de la infraestructura.

- Estructura de la Administración: Cambios en las responsabilidades de la administración que puedan afectar los controles que se llevan a cabo en la Entidad u Organismo.

- Personal: Calidad del personal contratado y los métodos de capacitación y motivación que puedan influir en el nivel de control de conciencia dentro de la Entidad u Organismo y vencimiento de contratos que puedan afectar la disponibilidad del personal.

- Acceso a los Activos: Naturaleza de las actividades de la Entidad u Organismo y acceso de empleados a los activos que puedan contribuir a la mala utilización de éstos.

- Procesos: Diseño y documentación de los procesos, conocimiento de entradas y salidas y capacidad de los procesos. Las fallas en los procesos son una causa recurrente que detona riesgos para la Entidad u Organismo.

- Tecnología: Alteraciones en los sistemas de información que puedan afectar los procesos y resultados de la Entidad u Organismo.

A continuación, se ejemplifican los riesgos de fuente externa e interna:

Ejemplos de riesgos de fuente externa

Ejemplos de riesgos de fuente interna

Así mismo, considerando el Principio 8 de las Normas Específicas de Evaluación de Riesgos de las Normas Técnicas de Control Interno (NTCI) emitidas por la Contraloría General de la República de Nicaragua, la Entidad u Organismo debe considerar los posibles actos irregulares, ya sean del personal de la Entidad u Organismo o de los proveedores de servicios externos que afectan directamente el cumplimiento de los objetivos. ***Ver Anexo N°. 3 Ejemplo de señales de alerta para actos irregulares.***

Ejemplos de posibles actos irregulares:

Las Entidades u Organismos de la Administración Pública deben diseñar respuestas a los riesgos por irregularidades, mediante el mismo proceso de respuesta desarrollado para todos los riesgos institucionales analizados. Esto posibilita la implementación de controles para el fortalecimiento de las buenas prácticas en la función pública, previniendo cualquier tipología de los delitos y fraudes contra la administración pública. Dichos controles pueden incluir la reorganización de ciertas operaciones y la reasignación de puestos entre el personal para mejorar la segregación de funciones.

Cuando estas irregularidades han sido detectadas, es necesario revisar el proceso de administración de riesgos. A estos riesgos de corrupción, fraude, abuso y otras irregularidades no les es aplicable el concepto de tolerancia al riesgo, ya que la incidencia de un acto corrupto implica necesariamente una deficiencia en los objetivos de cumplimiento legal. Para los objetivos de cumplimiento, la tolerancia al riesgo es

cero.

Contexto en el cual se Materializan los Riesgos
Es importante mencionar en qué contexto se materializan los riesgos, para identificar plenamente cada uno de los elementos que se encuentran presentes cuando ocurren. Es necesario diferenciar entre las causas y los efectos de un riesgo. Las causas definen el origen del riesgo y permiten identificar la esencia de lo que se considera como riesgo, mientras que los efectos son las consecuencias o resultados que las causas producen y tienen la característica particular de ser el detonador, para posteriormente cuantificar y medir el riesgo.

Ejemplo:

Riesgo: Un servidor público compra materiales de oficina innecesarios y además lo sustrae, para posteriormente obtener un beneficio personal.

Causa: Falta de segregación de funciones. Un servidor público de la Unidad de Adquisiciones tiene facultades para solicitar, tramitar y autorizar una compra de materiales.

Consecuencia: Pérdida económica para la Entidad u Organismo.

En síntesis, con la realización de esta fase la Entidad u Organismo estará en la posibilidad de obtener los siguientes resultados:

- Identificar los factores externos que pueden ocasionar la presencia de riesgos, con base en el análisis de la información externa, los planes y programas de la Entidad u Organismo.

- Identificar los factores internos que pueden ocasionar la presencia de riesgos con base en el análisis del ambiente de control y demás estudios que sobre la cultura organizacional y el clima laboral se hayan realizado en la Entidad u Organismo.

- Información que facilite las demás fases del Proceso de Gestión de Riesgo.

FASE 2: IDENTIFICACIÓN DE RIESGOS

La identificación de los riesgos debe efectuarse utilizando un proceso sistemático para incluir todos los riesgos de la organización. La idea es generar una lista de todos los eventos o circunstancias que podrían afectar a la Entidad u Organismo para luego a mayor detalle, identificar las posibles condiciones que puedan suscitarse.

Se pueden aplicar diferentes técnicas de identificación de riesgos, lo importante es considerar las causas y escenarios posibles de los eventos identificados. Es importante no omitir las causas significativas, para este efecto existen herramientas y

técnicas como: checklists (listas de chequeo o verificación), diagramas de flujo, brainstorming (lluvia de ideas), análisis de sistemas, análisis de escenarios, etc. El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión y los tipos de riesgos.

Identificación de Riesgos por Procesos.

El proceso de Gestión de Riesgos debe aplicarse a niveles de procesos, desagregados en sub procesos, actividades y riesgos específicos. En general el Proceso de Gestión de Riesgos se inicia con los procesos más críticos de la Entidad u Organismo, para ir ampliándose a una mayor cobertura, de manera de considerar todos los procesos que incidan en el logro de los objetivos de la organización gubernamental.

Esta técnica tiene las siguientes ventajas:

- Obliga al personal encargado de cada Unidad Organizativa a conocer e interactuar en forma integral con su organización.

- Permitir construir la Matriz de Riesgos de la Entidad u Organismo en materia especifica que se quiera analizar.

- Se genera una sólida base para aplicar y documentar el Proceso de Gestión de Riesgos.

- Una vez identificados los procesos que desarrolla la Entidad u Organismo se debe realizar la desagregación de procesos, la identificación de los riesgos y controles.

En caso que las Entidades u Organismos no cuenten con documentación formalizada de los procesos, subprocesos y actividades (manuales de procesos y procedimientos, normativas, entre otras), se debe revisar en conjunto con los directivos responsables la estructura de los procesos. Con esa información se analizará la relación entre los objetivos formales aprobados y los procesos organizacionales claves para el cumplimiento del objetivo. No obstante, por mandato de ley y de las Normas Técnicas de Control Interno emitidas por este Órgano de Control y Fiscalización, las Entidades y Organismos de la Administración Pública están taxativamente obligadas a la actualización permanente y desarrollo de todas las herramientas de gestión para la implementación de los controles internos.

A continuación, se expone un ejemplo de identificación de riesgos a través de un Diagrama de flujo. ***Anexo N°. 4.***

Para facilitar la identificación de los riesgos, los servidores de las Unidades Organizativas (áreas de gestión) de la organización, con la especialidad temática y la experiencia adquirida en cada sector o contexto en el que se desenvuelven,

efectuarán un inventario de los riesgos, que incluya la definición de las causas, la clasificación de la categoría y la identificación de la consecuencia o efecto, centrándose en los más significativos para la Entidad u Organismo, relacionados con el desarrollo de los procesos y los objetivos institucionales del área objeto de análisis.

Para este efecto se utilizará el ***Formato N°. 1 "Matriz de Identificación de Riesgos***" que podrá ser aplicado a nivel de Programa, Proyecto, Proceso o Actividad específica en cualquier Entidad u Organismo de la Administración Pública.

FASE 3: ANÁLISIS DE RIESGOS

El análisis de riesgos consiste en determinar la probabilidad de ocurrencia de los riesgos, así como su impacto, calificándolos con el fin de establecer el nivel de riesgo y las acciones que se requieren implantar.

Para el análisis del riesgo se requiere la información obtenida en el Formato "Matriz de Identificación de Riesgos" que se apoya en la disponibilidad de datos estadísticos, históricos e información generada en los sistemas de la Entidad u Organismo.

En la presente Guía se han establecido tres aspectos para tener en cuenta en el análisis de los riesgos identificados: **Importancia, Probabilidad e Impacto.**

Importancia del riesgo identificado está relacionada con la relevancia del factor en la gestión institucional.

Probabilidad es la posibilidad de ocurrencia del riesgo, que puede ser medida con criterios de Frecuencia (por ejemplo, número de veces en un tiempo determinado) o *Factibilidad*, teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo.

Impacto se entiende como las consecuencias del riesgo o la magnitud de sus efectos en caso que se materialice.

Los riesgos se calificarán usando métodos cualitativos y cuantitativos, con un doble enfoque: Riesgo inherente y Riesgo residual.

El Riesgo inherente, es aquél al que se enfrenta una entidad en ausencia de acciones de los directivos para modificar su probabilidad o impacto.

El Riesgo residual, es el riesgo remanente después de que la administración lleva a cabo sus respuestas o acciones para mitigar, reducir, trasladar o compartir los riesgos.

La magnitud del impacto y la probabilidad de ocurrencia de los riesgos se analizan en el contexto de los controles existentes.

Probabilidad, impacto e importancia se combinan para obtener el nivel de riesgo inherente.

La probabilidad e impacto pueden determinarse utilizando análisis y cálculos estadísticos, datos anteriores (históricos), inclusive se pueden realizar estimaciones que reflejen el grado de convicción de un individuo o grupo de que podrá ocurrir un evento o resultado particular.

Con la finalidad de evitar juicios de valor subjetivos, deben utilizarse las mejores técnicas y fuentes de información disponibles, por ejemplo, se deberán revisar registros anteriores, prácticas y experiencia de la actividad, investigaciones de mercado, opiniones de especialistas y expertos, entrevistas, cuestionarios, información de fallas o inconformidades en los productos o servicios, etc.

En la calificación de riesgos se introduce el concepto de Importancia con la finalidad de distinguir el grado de relevancia del factor de riesgo en la gestión institucional, y se determinará con la siguiente tabla:

Para determinar de manera objetiva la **Probabilidad**, en la presente Guía se utilizará la tabla siguiente:

Para determinar el **Impacto** se utilizará la tabla siguiente:

El impacto puede expresarse de varias formas según la característica de los factores de riesgo analizados, por ejemplo: impacto de confidencialidad de la información, impacto de credibilidad, impacto financiero, impacto en la salud o seguridad del personal, etc.

A continuación, se presenta un cuadro con el cálculo de todas las posibilidades de calificación al combinar estos tres aspectos: importancia, probabilidad e impacto:

Calificación del Riesgo

Se procederá a calificar cada uno de los factores de riesgo identificados, según las especificaciones indicadas anteriormente: importancia, probabilidad e impacto, cuyos resultados permitirán calificar los riesgos en BAJO, MEDIO Y ALTO y proveer datos importantes para las siguientes fases: evaluación y tratamiento de los riesgos.

La escala para la calificación del riesgo como: *Bajo, Medio y Alto*, se representará con los colores siguientes:

En la Matriz de riesgos, se procederá a la calificación de los tres aspectos: importancia, probabilidad e impacto y se multiplicaran estos tres aspectos obteniendo el resultado de la calificación final del riesgo inherente; en este nivel de análisis se considera que la administración no ha establecido controles. Ver ***Formato N°. 2 "Matriz, de Análisis y Calificación de Riesgos".***

FASE 4: EVALUACIÓN DE RIESGOS

La evaluación de los riesgos permite a una Entidad considerar la amplitud con que los eventos potenciales impactan en la consecución de objetivos.

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgos establecidos previamente por la Dirección, considerando el balance entre los beneficios potenciales y resultados adversos.

El control es una etapa primordial en la administración, aunque una Entidad u Organismo tenga excelentes controles, una estructura organizacional adecuada y una dirección eficiente, es necesario que exista un mecanismo que verifique e informe si los hechos y actividades de la Entidad u Organismo se están desarrollando según los objetivos.

La administración deberá identificar los sistemas y procedimientos existentes para controlar los riesgos. Se pueden utilizar entre otros: listas de chequeo, diagramas de flujo, análisis de sistemas, así como inspecciones y técnicas de autoevaluación de controles.

Valoración del Riesgo[11]

[11] Cartilla de Administración Pública, Departamento Administrativo de la Función Pública República de Colombia, Escuela Superior de Administración Pública, Guía de Administración del Riesgo

La valoración del riesgo se obtiene al comparar los resultados de la evaluación del riesgo con los controles existentes establecidos en los diferentes procesos por la entidad.

Las Actividades de Control pueden ser:

Preventivos: Son diseñados para evitar eventos no deseados, y actúan para eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.

Detectivos o Correctivos; Son diseñados para detectar y descubrir eventos no

deseados después que han ocurrido. Permiten el restablecimiento de la actividad después de haber detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

Manuales, automatizados o informatizados: De acuerdo a la complejidad y características específicas del riesgo a mitigar.

Gerenciales y Operativos: Las Actividades de Control Gerenciales son diseñadas para determinar en qué medida se están alcanzando los objetivos de la Entidad u Organismo y detectar eventos relevantes para la oportuna toma de decisiones. Mientras que las Operativas, son diseñadas para mitigar de manera específica eventos que se desarrollan en su área de competencia de acuerdo a sus responsabilidades y autoridad.

Identificados los riesgos, es necesario describir y analizar los controles claves existentes en la Entidad u Organismo, los que teóricamente mitigan los riesgos, es decir todas las medidas que ha tomado la administración con la finalidad de evitar la ocurrencia de un riesgo potencial. Estos controles deben ser evaluados en el nivel de cumplimiento de los elementos de un control adecuado y calificados de acuerdo a su diseño, es decir, su oportunidad (en qué momento del proceso se aplican: preventivos, correctivos, detectivos), periodicidad (si son permanentes, periódicos u ocasionales), grado de automatización (manual, semi automatizado, automatizado) y evaluados en términos de cumplimiento de normas específicas de control.

Los controles deben ser identificados con una descripción del mismo que contenga al menos los antecedentes siguientes:

- ¿Qué actividad se realiza?

- ¿Cómo se ejecuta el control?

- ¿Quién es el responsable?

- ¿Cuándo ejecutan el control?

Ejemplo:

- Restricciones de Acceso **(Qué se realiza)**.

- Existe una restricción de acceso a la sala de servidores, debido a que sólo pueden ingresar el personal que tiene tarjeta especial y clave de acceso, la cual sólo se entrega a tres funcionarios responsables de la División de Sistemas **(Cómo se realiza el control).**

- La emisión de tarjeta de autorización para el acceso y la entrega de claves se

realizan por el Jefe de la División de Sistemas, previa aprobación del Jefe de Servicio de los funcionarios habilitados **(Quién lo realiza).**

- Las autorizaciones son revisadas mensualmente por el Jefe de la División de Sistemas, que emite un reporte al Jefe de Servicio **(Cuándo lo ejecuta).**

El procedimiento de valoración de riesgo

Para realizar la evaluación de los controles existentes es necesario describirlos, estableciendo si son preventivos o correctivos y responder a las preguntas siguientes:

- ¿Los controles están documentados?

- ¿Se están aplicando en la actualidad?

- ¿Son efectivos para minimizar el riesgo?

Una vez que se ha respondido estas preguntas, se procede a realizar la valoración así:

- Calificados y evaluados los riesgos analícelos frente a los controles existentes en cada riesgo, para identificar en qué medida la Entidad u Organismo está gestionando los riesgos.

- Pondérelos según la tabla establecida, teniendo en cuenta las respuestas a las preguntas anteriormente formuladas (los controles se encuentran documentados, se aplican y son efectivos).

- Ubique en la matriz de evaluación el estado final del riesgo, de acuerdo a los resultados obtenidos en la valoración del mismo.

En los siguientes cuadros se pueden observar ejemplos de distintos tipos de control:

Un control adecuado es el que está presente si la Dirección ha planificado y organizado (diseñado) las operaciones, de manera que proporcionen un aseguramiento razonable de que los objetivos y metas de la organización serán alcanzados de forma eficiente y económica.

En consideración a lo anterior, un control para poder ser declarado como adecuado debe tener las siguientes propiedades:

- Permitir la corrección de fallas y errores: El control debe detectar e indicar errores de planeación, organización o dirección.

- Contribuir a la prevención de fallas o errores futuros: El control, al detectar e indicar

errores actuales, debe prevenir errores futuros, ya sean de planeación, organización o dirección.

El Riesgo Residual permanece después de que la Dirección desarrolla sus respuestas al riesgo o después que ha establecido controles.

El Riesgo Residual es el resultado de la multiplicación de los valores de la importancia, nuevos valores de la probabilidad e impacto si procede, considerando los controles existentes. El valor otorgado a la importancia se mantiene igual para el cálculo del Riesgo Residual. Para el cálculo de la probabilidad e impacto se considera las mismas tablas de la Fase III. Análisis de Riesgo.

Así mismo en la Matriz de Evaluación de Riesgos se identificará el Riesgo Residual de color verde (riesgo bajo), amarillo (riesgo medio) o rojo (riesgo alto) que se podrá visualizar en el ***Formato N°. 3 "Matriz de Evaluación de Riesgos".***

Para realizar la evaluación se debe tomar en cuenta la calificación obtenida en cada riesgo, si el riesgo es **Bajo,** significa que su posibilidad de ocurrencia es improbable y su impacto es *bajo*, lo cual permite a la entidad asumirlo; quiere decir que el riesgo se encuentra en un nivel que se puede aceptar sin necesidad de tomar otras medidas de control diferentes a las que existen y que su grado de importancia es *bajo.*

Si el riesgo es calificado como **Medio o Alto**, significa que la posibilidad de ocurrencia es probable o muy probable, que su impacto es medio o alto; por tanto, es aconsejable eliminar la actividad que genera el riesgo en la medida que sea factible. De lo contrario, se deben implementar controles de prevención para evitar su ocurrencia e impacto, compartir o transferir el riesgo a través de otras opciones.

En los casos en que el riesgo es calificado como Medio o Alto, se deben tomar medidas para llevar en lo posible los riesgos a la calificación Baja, y cuando el riesgo sea Alto a pesar de estas acciones, la Entidad u Organismo deberá optar por diseñar planes de contingencia para protegerse de su ocurrencia.

Con la realización de la valoración de los riesgos, la Entidad u Organismo obtiene los siguientes resultados:

- La identificación de los controles existentes para los riesgos identificados y analizados.

- La priorización de los riesgos de acuerdo con los resultados obtenidos al confrontar la evaluación del riesgo con los controles existentes y obtener la calificación del Riesgo Residual.

- Establecer los riesgos que pueden causar mayor impacto a la Entidad u Organismo en caso de materializarse.

FASE 5: GESTIÓN O TRATAMIENTO DE LOS RIESGOS

Una vez evaluados los riesgos relevantes, se determina cómo responder a ellos.

El tratamiento de los riesgos consiste en identificar las opciones para mitigarlos, su valoración y la implementación del plan para llevarlas a cabo. Dichas opciones se refieren a las oportunidades que tiene la Entidad para disminuir el nivel de riesgo, de acuerdo con las prioridades establecidas en la Fase de evaluación.

Por esta razón, es conveniente para la Entidad u Organismo que en la selección de las opciones se tenga en cuenta en lo posible su aplicación a los diferentes riesgos, a fin de buscar soluciones combinadas y estrategias globales. Igualmente, es pertinente analizar el costo beneficio de la gestión del riesgo para tomar la mejor decisión.

Alternativas de Mitigación del Riesgo

Las alternativas de mitigación pueden ser: **evitar o anular, reducir, compartir y aceptar el riesgo.**

- **Evitar o Anular el riesgo**, donde evitar significa tomar las acciones encaminadas a prevenir su materialización y anular significa la salida de actividades que dan lugar a riesgos. Evitar es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y actividades emprendidas. Un ejemplo de esto puede ser el control de calidad, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

Sólo se anula un riesgo cuando se elimina la actividad, si fuera esto posible para la Entidad u Organismo.

- **Reducir el riesgo**, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

- **Compartir o transferir el riesgo**, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, por ejemplo, en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

Cuando los riesgos son total o parcialmente transferidos, la organización que transfiere

los riesgos ha adquirido un nuevo riesgo, que la organización a la cual ha transferido el riesgo no pueda administrarlo efectivamente.

- **Aceptación del riesgo**, luego de que el riesgo ha sido reducido o transferido puede quedar un Riesgo Residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.[12]

[12] Cartilla de Administración Pública, Departamento Administrativo de la Función Pública República de Colombia, Escuela Superior de Administración Pública, Guía de Administración del Riesgo.

En el siguiente esquema se resume el proceso de tratamiento de los riesgos: [13]

[13] AS/NZS 4360:1999, Estándar Australiano, Administración de Riesgos

Los planes de mitigación o tratamiento de los riesgos deben incluir por lo menos los siguientes aspectos: identificación del proceso o proyecto, definición del riesgo, las actividades propuestas, los recursos necesarios, los responsables y cronogramas de ejecución, así como la evidencia de cumplimiento a través de los cuales se medirá la mitigación del riesgo. ***Formato N°. 4 "Plan de Mitigación o Tratamiento de los Riesgos".***

El propósito de los planes de mitigación o tratamiento de los riesgos, es documentar la forma en que se van a implementar las opciones (evitar o anular, compartir, reducir y aceptar) con requisitos de presentación de informes y monitoreo.

Es importante mencionar que el éxito en la ejecución de los planes de mitigación o tratamiento de los riesgos, depende en muchos casos de la aceptación y conocimiento de las personas involucradas, por lo que lograr su cooperación y participación es fundamental. Lo ideal es que la responsabilidad del riesgo sea llevada a cabo por aquellos con mayor posibilidad de controlar el riesgo.

Un plan de mitigación o tratamiento de los riesgos es más objetivo cuando se han identificado claramente las causas internas o externas del factor de riesgo, porque de ello depende el grado de control que puede aplicarse y por consiguiente la efectividad del tratamiento.

La implantación del plan de mitigación o tratamiento de los riesgos es exitosa cuando se definen claramente los métodos seleccionados, se asignan responsabilidades individuales en las acciones y se monitorean periódicamente.

A continuación, se presentan ejemplos de respuesta al riesgo en las categorías correspondientes desarrollados en el marco integrado de COSO[14]

[14] Administración de Riesgos Corporativos - Marco Integrado, Técnicas de Aplicación, Diciembre de 2005, Price Waterhouse&Coopers, COSO (The Committe of Sponsoring Organizations of the Treadway Commission), FLAI (Federación Latinoamericana de Auditores Internos. y ampliados en el documento Implantación, mantención y actualización del Proceso de Gestión de Riesgo en el sector público[15]

[15]Documento Técnico No. 70, versión 0.2 Implantación, mantención y actualización del proceso de gestión de riesgo en el sector público, del Consejo de Auditoría Interna General del Gobierno de Chile, Año 2016.

Si luego del tratamiento hay un Riesgo Residual, se debe tomar la decisión de aceptar ese riesgo o repetir el proceso de tratamiento.

FASE 6: MONITOREAR Y REVISAR

La administración de riesgos institucionales se monitorea mediante actividades permanentes de los componentes, evaluaciones independientes o una combinación de las dos técnicas. El alcance y la frecuencia de las evaluaciones independientes dependen de la evaluación de los riesgos y la eficacia de los procedimientos de monitoreo permanente.

Es necesario monitorear todas las etapas del proceso de gestión de riesgo, para aplicar y sugerir los correctivos y ajustes necesarios que aseguren su efectivo manejo.

Los riesgos y la efectividad de las medidas de control requieren ser monitoreados para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos, éstos no son estáticos, pueden cambiar los factores que podrían afectar las probabilidades y consecuencias de un resultado, por lo tanto es indispensable revisar el ciclo de administración de riesgos en forma constante.

Una vez diseñado y aprobado el plan de mitigación de los riesgos, es preciso monitorear la ejecución de las actividades previstas para evaluar la eficiencia de su implementación e identificar sobre la marcha las situaciones o factores que pueden influir en la aplicación de las acciones de prevención.

A continuación, se detallan actividades para controlar los planes de tratamiento y monitoreo:

- Efectuar el seguimiento de las estrategias seleccionadas (evitar o anular, reducir, compartir y aceptar) y monitorear las actividades previstas en el plan de tratamiento.

- Verificar en forma trimestral el avance en la implementación del tratamiento de los riesgos.

- Analizar y evaluar los controles existentes, para mitigar los riesgos.

El Encargado de Riesgos (Área Organizativa de Planificación o el área que determine la máxima autoridad) y los Responsables de Riesgos (Responsables de Unidades Organizativas), como servidores responsables del monitoreo, deberán obtener información relevante de los sistemas de información y registros; establecerán estructuras de reportes e informarán a los niveles de decisión, en forma oportuna y periódica sobre el estado de los riesgos en cualquier fase del proceso; la finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar una adecuada gestión del riesgo.

A continuación, se presenta una lista básica de la información que debe ser incluida en los reportes de revisión y monitoreo:

- Período (fecha) de revisión o evaluación de las actividades.

- Reportes de revisiones periódicos para reducir los riesgos de errores o irregularidades.

-Reportes de monitoreo del entorno interno y externo.

- Resultados de la medición del cumplimiento de los objetivos.

- Evidencia del cumplimiento de los objetivos.

- Proyecciones de cumplimiento de los objetivos.

- Recomendaciones para que se obtenga el logro de los objetivos y se mejore en términos de oportunidad y calidad.

FASE 7: COMUNICAR Y CONSULTAR

Una comunicación efectiva interna y externa en todas las fases del proceso, con los servidores responsables de implementar la administración de riesgos y con los grupos de interés relacionados con las operaciones de la Entidad u Organismo, es fundamental para lograr coordinar las acciones y tomar las mejores decisiones en el manejo de riesgos.

Es importante desarrollar un plan de comunicación y consulta tanto para las partes involucradas internas como externas en las primeras etapas del proceso. Este plan debería abordar temas relacionados con el riesgo en sí y con el proceso para gestionarlo. Lo anterior se desarrolla con el objetivo de asegurar que los responsables

de implementar la gestión del riesgo y los directamente interesados entiendan la base sobre la cual se toman las decisiones y el porqué de las acciones particulares requeridas.

Es útil un enfoque de equipo consultivo para facilitar la definición adecuada del contexto, asegurar la eficaz identificación de los riesgos, para unir diferentes áreas de experiencia en el análisis de los mismos y así asegurar que se tienen diferentes puntos de vista sobre ellos y la adecuada gestión durante el tratamiento.[16]

[16] Norma Técnica Colombiana NTC 5254 Gestión del Riesgo.

El propósito es que los servidores responsables del servicio público y los terceros relacionados con la Entidad u Organismo estén informados de la marcha del Proceso de Gestión de Riesgos y la forma cómo se van implementando las actividades de mitigación de los mismos. Para ello es importante contar con informe y sistemas de información que generen de manera oportuna datos suficientes, confiables y completos para posibilitar una comunicación y control eficaz.

En consideración a que el objetivo fundamental de esta fase es obtener información confiable en todas las fases del Proceso de Gestión de Riesgos, en primer lugar, se debe elaborar o actualizar Planes de Comunicación y Consulta, adaptados a la realidad de la organización, considerando como mínimo los siguientes componentes y antecedentes:

1. Componente: Temas Relativos al Riesgo

Entre los antecedentes que se pueden considerar están:

- Reportes de análisis de indicadores relacionados con el Proceso de Gestión de Riesgos en general.

- Reportes de análisis relacionados con la Matriz de Riesgos.

-Reportes de actualización del análisis de riesgos.

- Reportes del Plan de Mitigación o Tratamiento de Riesgos.

En la Entidad u Organismo el Encargado de Riesgos (Área de Planificación o el área que determine la máxima autoridad) y los Responsables de Riesgos (Responsables de Unidades Organizativas), deberán monitorear en el mes de enero de cada año los cambios de estos resultados y así obtener información oportuna que ayude a la toma de decisiones de la máxima autoridad.

Algunos ejemplos de criterios e indicadores que la Entidad u Organismo consideren diseñar de acuerdo a su naturaleza y necesidades, en relación al análisis de la

información derivada del Proceso de Gestión de Riesgos:

Ejemplos de Criterios e Indicadores para Análisis de Información del Proceso de Gestión de Riesgos

2. Componente: Realizar Comunicaciones y Consultas Internas y Externas Eficaces

El objetivo es asegurarse que los responsables de la implementación del Proceso de Gestión del Riesgo y las partes interesadas en la organización comprenden las bases que han servido para tomar decisiones y las razones por las que son necesarias determinadas acciones. Entre los antecedentes se consideran:

- Identificar usuarios o clientes internos y externos, y su nivel de importancia para el Proceso de Gestión de Riesgos.

- Definir qué tipo de información se espera recibir y remitir en el proceso.

- Definir roles y responsables de la calidad y confiabilidad de la información a recibir y remitir.

- Definir periodicidad para recibir y remitir información.

- Identificar y definir sistemas, canales y mecanismos para manejar la información de gestión de riesgos al interior de la organización y para remitirla externamente.

- Definir qué tipo de reportes tendrá el proceso. Definir tipo de análisis que se incluirán en los reportes.

- Definir quiénes y cómo tendrán acceso a la comunicación, señalando los criterios para definir perfiles por tipo de información.

- Definir como se recolectarán opiniones que genere la comunicación y espacios de participación.

Posteriormente, se deberá analizar a una fecha dada, los resultados de la aplicación de los Planes de Comunicación y Consulta y emitir un informe. Solicitar a los usuarios de la información contestar algunas de las siguientes preguntas relacionadas con el contenido, oportunidad, actualidad, exactitud y accesibilidad de los reportes internos y externos, puede ser de utilidad para esta tarea. Entre otros se consideran las siguientes:

- En relación al contenido. ¿Contiene toda la información necesaria?

- En relación con la oportunidad. ¿Se facilita en el tiempo adecuado?

- En lo relativo a la actualidad. ¿Es la más reciente disponible?

- En relación con la exactitud. ¿Los datos son correctos?

- Por último, en relación a la accesibilidad. ¿Puede ser obtenida fácilmente por las personas adecuadas?

X. DISPOSICIONES FINALES

Divulgación. Es responsabilidad de la División General de Investigación, Desarrollo y Capacitación Aplicada, divulgar el contenido de la presente Guía Especializada para la Evaluación de Riesgos en el Sector Público, al personal que participa en el proceso de evaluación de riesgos en las Entidades y Organismos de la Administración Pública.

Uso y Cumplimiento. Las máximas autoridades, administración y demás servidores públicos de las Entidades y Organismos, están obligados a la implementación y cumplimiento de las disposiciones contenidas en la presente Guía.

Derogación. Deróguese la Guía Especializada de Control Interno en Evaluación de Riesgo, aprobada el 21 de junio de 2012, en sesión ordinaria No. 786, del Consejo Superior de la Contraloría General de la República.

Modificación y Actualización. La presente Guía podrá ser modificada o actualizada por la División General de Investigación, Desarrollo y Capacitación Aplicada, la que posteriormente será aprobada por la máxima autoridad administrativa de la Contraloría General de la República.

Vigencia. La presente Guía Especializada para la Evaluación de Riesgos en el Sector Público, entrara en vigencia a partir del primero de enero del año dos mil veintitrés previa publicación en la Gaceta, Diario Oficial y en el sitio web de la Contraloría General de la República.

XI. ANEXOS Y FORMATOS

Anexos

N°. 1 Vinculación de los Objetivos Estratégicos, Operativos y Específicos.

N°. 2 Etapas para la Implementación de la Administración de Riesgos.

N°. 3 Ejemplo de Señales de Alerta para Actos Irregulares.

N°. 4 Análisis del Flujo de Procesos con la Identificación de Eventos.

Formatos

N°. 1 Matriz de Identificación de Riesgos

N°. 2 Matriz de Análisis y Calificación de Riesgos

N°. 3 Matriz de Evaluación de Riesgos

N°. 4 Plan de Mitigación o Tratamiento de los Riesgos

Instructivo para las Matrices del N°. 1 al 4

Anexo N°. 1 Vinculación de los Objetivos Estratégicos, Operativos y Específicos

Fuente: Informe de Evaluación de la Gerencia de Planificación y Presupuesto del Registro Nacional de Identificación y Estado Civil RENIEC, Perú.

Anexo N°. 2 Etapas para la Implementación de la Administración de Riesgos

Las principales etapas para lograr la implementación de la administración de riesgos son las siguientes:

1) Preparación del Equipo - con representación y funciones claves, que diseñe e implante un proceso de administración de riesgos, que aborde las necesidades específicas de la Entidad u Organismo.

2) Apoyo de la Máxima Autoridad - de forma oportuna, establezca la Política de Riesgo, la designación de la estructura para la implementación de la gestión de riesgos, los canales de comunicación, la disponibilidad de los recursos y el seguimiento a la efectividad de la aplicación del Plan de Mitigación y Tratamiento de Riesgos.

3) Desarrollo del Plan de Implementación - que incluya las fases, hitos, recursos y calendario; responsables de la comunicación y coordinación del equipo a las diversas unidades organizativas y personas para gestionar la adopción de la administración de riesgos.

El Plan debe contemplar los riesgos a los que se encuentra expuesta la Entidad u Organismo y las actividades para mitigarlos.

4) Desarrollo y Comunicación de la Política Organizacional - para asegurar que la administración de riesgos se convierta en parte integral de los procesos y de la cultura institucional.

5) Administración de los Riesgos a Nivel Organizacional - a través del cumplimiento de todas las fases del Proceso de Gestión de Riesgos, mediante el establecimiento de mecanismos de comunicación oportuna.

6) Administración de los Riesgos a Nivel de Proyecto, Actividad o Proceso - por cada área de gestión o unidad administrativa

7) Monitoreo y Mejora Continua - seguimiento y evaluación de la implementación del proceso de gestión de riesgos para revisar su efectividad y reforzar las capacidades de la Entidad u Organismo como parte del proceso continuo de mejoramiento, de tal manera que los riesgos no sean estacionarios.

Anexo N°. 3 Ejemplo de Señales de Alerta para Actos Irregulares

Las señales de alerta de delitos se pueden concebir como: indicadores, indicios, condiciones, comportamientos, alertas tempranas o banderas rojas de ciertas operaciones o personal que podrían permitir potencialmente detectar la presencia de una operación inusual, que conlleve a una mayor investigación.

Es de vital importancia que las Entidades u Organismos, en base a la identificación y análisis de riesgos asociados generen sus propias señales de alerta, que les permitirá fortalecer el sistema de prevención de delitos implementado en la Entidad u Organismo.

A continuación, se mencionan a manera de ejemplo, señales de alerta genéricas, que se pueden identificar en las actividades operativas en cualquier tipo de Entidad u Organismo y que pueden ser indicativas, debiendo examinarse debidamente para ver si corresponden a situaciones anómalas. Sin perjuicio de lo anterior, las señales de alerta, siempre deben ser identificadas y analizadas de acuerdo al contexto del sector donde está incorporada la Entidad u Organismo.

1. Asociadas a la probidad funcionaría

- Recibir en el cumplimiento de sus funciones públicas, donaciones, regalos o cualquier otro bien o servicio bajo cualquier concepto, proveniente de personas naturales o jurídicas.

- Uso de fondos públicos para actividades o compras ajenas a la Entidad u Organismo.

- Uso de fondos públicos para compras de regalos o donaciones que no estén autorizadas por ley.

1. Asociadas a conflictos de interés

- Servidores públicos que ejercen cargos de directores o ejecutivos de una entidad jurídica y que participan directa o indirectamente de una licitación o contrato en la Entidad.

2. Asociadas a manejo de información

- Otorgamiento de privilegios o permisos distintos al perfil del usuario de una cuenta, o a usuarios no autorizados.

- Servidor público que divulga información personal de otros servidores de su organización gubernamental a empresas que manejan bases de datos.

- Servidor Público que revela, de forma ilegal, información confidencial a determinada (s) empresa (s), en el marco de una licitación pública.

- Existencia de evidencias que soportan el sabotaje en el uso de claves de acceso para el ingreso a los sistemas.

- Existencia de evidencias que soportan un posible ocultamiento de la información y/o cambio intencional de la información reportada.

3. Asociadas a Inventarios

- Movimientos de inventarios duplicados.

- Programas de inventarios donde los usuarios pueden modificar los datos.

- Ingreso o salida de productos inexistentes físicamente.

4. Asociadas a transacciones financieras utilizando fondos públicos

- Depósito frecuente de cheques girados desde cuentas de Entidades u Organismos que son depositados en cuentas particulares y que inmediatamente son retirados o transferidos.

- Pagos a la orden de una empresa o persona distinta del proveedor.

- Arreglos especiales con bancos para establecer transacciones poco claras (giros, préstamos, etc.).

- Ausencia, alteración o simulación de documentos que soportan el origen de las transacciones financieras relacionadas con la Entidad u Organismo.

- Solicitudes de pagos de último momento, sin el suficiente respaldo documental.

- Ruptura de la secuencia numérica de los cheques.

5. Asociadas al pago de remuneraciones

- Depósitos de sueldos en cuentas bancarias a nombre de un beneficiario distinto del personal.

- Pagos a servidores fantasmas (empleados inventados), sueldos ficticios o duplicados.

- Pagos realizados a servidores públicos por conceptos distintos a los estipulados para sus remuneraciones.

6. Asociadas a compras

- Fragmentación de licitaciones y/o contratos por motivos injustificados y repetitivos.

- Otorgar contratos a proveedores en razón de la existencia de lazos de parentesco consanguíneo o por afinidad en cualquiera de sus grados.

- Presentación de varias propuestas idénticas en el proceso de adquisición.

- Adjudicación del contrato a un proponente que no cumple con los requisitos solicitados en las bases de licitación publicadas.

- Presentación de propuestas y/o adjudicación de contratos por valores significativamente mayores o inferiores a los precios de mercado de los bienes o servicios en cuestión.

- Marcado interés de algún funcionario evaluador por una propuesta en particular, cuando existan otras propuestas en igualdad de condiciones.

- Sospechas relacionadas con solicitudes de sobornos o coimas realizadas para avalar estudios o emitir opiniones técnicas favorables a un proponente, por parte de la persona relacionada al proceso de contratación.

- Crecimiento excesivo e injustificado de las cuentas por cobrar de la Entidad u Organismo, con respecto al comportamiento de los mismos en rubros en periodos anteriores.

- Diferencias entre orden de compra, informes de recepción y factura por proveedor, entre esta última y la orden de pago.

- Existencia de evidencias que soportan que se ha realizado alteración de facturas y adulteración de documentos.

- Ruptura de la correlatividad en la numeración de las órdenes de compra, informes de recepción y órdenes de pago.

Anexo N°.4 Análisis del Flujo de Procesos con la Identificación de Eventos [17]

[17] The Committee of Sponsoring Organizations of the Treadway Commission, Administración de Riesgos Corporativos, Marco Integrado, Técnicas de Aplicación, páginas 31-32.