ASF Auditoría Superior de la Federación

CÁMARA DE DIPUTADOS

Guía de Autoevaluación de Riesgos en el Sector Público

AUDITORÍA ESPECIAL DE TECNOLOGÍAS DE INFORMACIÓN, COMUNICACIONES Y CONTROL

Índice

Introducción

A lo largo de 2013 y 2014, la Auditoría Superior de la Federación (ASF) trabajó con las instituciones del sector público federal con objeto de contribuir al fortalecimiento de sus sistemas de control interno y de sus programas de promoción de la integridad. Para ello, utilizó un enfoque basado en la aplicación de evaluaciones especializadas y la difusión de mejores prácticas en la materia.

La ASF tiene la convicción de que la mejora del control interno es uno de los ejes indispensables para elevar la eficiencia y economía de la gestión pública, así como un elemento imprescindible para reducir efectivamente la posibilidad de ocurrencia de actos corruptos desde un enfoque preventivo, disciplinado y sistemático.

En las más de 400 reuniones de facilitación relativas al control interno y la salvaguarda de la integridad que la ASF sostuvo en 2014 con más de 190 instituciones federales, se hizo patente la necesidad que existe en un número significativo de ellas de contar con herramientas metodológicas especializadas, las cuales les permitan evaluar los riesgos que enfrentan en el logro de sus objetivos.

Como respuesta a esa necesidad, expresada de manera recurrente por múltiples instituciones, y como una contribución al Sistema Nacional de Fiscalización (SNF), la ASF presenta esta *Guía de Autoevaluación de Riesgos en el Sector Público*, la cual está concebida para ser utilizada por toda institución de gobierno que así lo decida, independientemente del Poder en que se encuentre y el orden de gobierno al que pertenezca. Debe señalarse que la legislación vigente en materia de administración de riesgos no se encuentra homologada a nivel nacional; incluso en el orden federal, los distintos Poderes cuentan con marcos regulatorios distintos y, en algunos casos, inexistentes.

Por esa razón, la presente guía ha sido preparada tomando en consideración el marco normativo que sí se encuentra vigente y es por tanto obligatorio para determinadas instituciones, al tiempo que es un documento de orientación para aquellas instituciones que no cuentan con normas específicas en relación con la gestión de riesgos.

En otras palabras, la puesta en práctica de esta guía permitirá a las instituciones cumplir cabalmente con sus obligaciones de administración de riesgos en caso de que se encuentren normadas en dicha esfera. A la vez será una herramienta útil para el establecimiento de tal actividad en las organizaciones que, aun sin estar sujetas a una regulación específica, se ven impelidas a gestionar sus riesgos como parte de una modernización y mejora continua.

Por ello, para la elaboración de esta guía no sólo se analizó la legislación federal y local respectiva, a efecto de hacerla compatible; también se tomaron en consideración las mejores prácticas internacionales en la materia, como son las Normas de las Entidades Fiscalizadoras Superiores publicadas por la INTOSAI, las normas del Instituto Internacional de Auditores Internos y los lineamientos establecidos en la materia por el Modelo COSO 2013, entre otras reconocidas fuentes internacionales.

Es importante observar que, además de preparar esta guía, la ASF ha desarrollado la herramienta tecnológica "Sistema Automatizado de Administración de Riesgos", la cual también pone a disposición de todas las instituciones gubernamentales.

Dicha herramienta tiene como propósito que todo ente del sector público esté en posibilidad de realizar el registro de los riesgos que enfrenta, evaluarlos conforme a su impacto y probabilidad de ocurrencia, asignar responsables específicos, obtener los mapas respectivos y, en breve, hacer de la administración de riesgos una realidad funcional en la operación cotidiana de la institución.

Desde la perspectiva de la fiscalización superior, muchas de las dificultades que enfrenta la gestión pública —y que han sido un factor de erosión de la confianza en la capacidad del Estado para resolver las demandas ciudadanas más urgentes— pueden ser abordadas desde enfoques técnicos que han demostrado su utilidad y eficacia en donde se han implantado.

Para la ASF, tanto las reuniones de facilitación sostenidas, como la preparación de diversas guías especializadas y la elaboración de la herramienta automatizada para la administración de riesgos, representan una serie de contribuciones técnicas y especializadas para la mejora general de la gestión pública, al tiempo que se traducen en un ahorro sustantivo de recursos económicos para las instituciones que decidan implementarlas.

Con la publicación de esta guía, el órgano de fiscalización superior federal respalda su compromiso de seguir consolidando el Sistema Nacional de Fiscalización como una pieza clave para fortalecer el desempeño gubernamental, y de que continúe brindando beneficios a sus miembros y a las instituciones del país para trabajar con mayores niveles de control interno, integridad, transparencia y rendición de cuentas.

A quién está dirigida la Guía

La Guía de Autoevaluación de Riesgos en el Sector Público está estructurada para que pueda ser aplicada por todo tipo de instituciones gubernamentales de cualquier Poder de la Unión y orden de gobierno al que pertenezcan, sin contravenir su mandato ni características particulares, ya que contiene los principios fundamentales para una administración de riesgos efectiva y está elaborada con base en la legislación nacional aplicable, así como en las mejores prácticas internacionales en esta materia.

Los resultados del Estudio General sobre la Situación que Guarda el Sistema de Control Interno en el Sector Público Federal (1172) y del Estudio Técnico para la Promoción de la Cultura de Integridad en el Sector Público (1173), los cuales fueron publicados en el Informe del Resultado de la Fiscalización Superior de la Cuenta Pública 2012, reflejan que gran parte de las instituciones estudiadas (ver cuadro 1), se encuentran en un nivel básico de madurez respecto de la implantación y funcionamiento de su sistema de control interno e integridad. De igual modo, se ha hecho manifiesta en algunas instituciones la carencia de herramientas técnicas de aplicación práctica para llevar a cabo una adecuada administración de riesgos.

Con base en lo anterior y otros factores detectados en ambos Estudios, surgió la necesidad de diseñar y poner a disposición del sector público, en sus tres órdenes de gobierno, este instrumento metodológico, con la finalidad de reforzar y enfocar los esfuerzos de fortalecimiento de los sistemas institucionales de control interno. En particular, el presente documento está orientado en identificar, evaluar, analizar, responder, controlar, supervisar y comunicar los riesgos que en caso de materializarse puedan provocar efectos negativos respecto del logro de los objetivos y metas institucionales.

Resultados del Componente Evaluacción de Riesgos en las instituciones del Poder Ejecutivo Federal

Número de Instituciones	Programa/Plan Estratégico		Identificacación de Riesgos Institucionales		Procedimiento para la Administración de Riesgos		Metodología para la Administración de Riesgos		Evaluación de Riesgos en Procesos Susceptibles a Actos de corrupción	
	Si	No	Si	No	Si	No	Si	No	Si	No
279	149	130	161	118	66	213	110	169	4	275
%	53%	47%	58%	42%	24%	76%	39%	61%	1%	99%

Cuadro 1. Fuente: Elaborado por la ASF con información del Estudio 1172.

Tipología de riesgos

Existen diferentes tipos de riesgos, los cuales se clasifican de acuerdo con su naturaleza, como se muestra en el cuadro siguiente:

Tipología de Riesgos	
Discrecionales	No discrecionales
Resultan de la toma de una posición de riesgo	Resultan de la operación de la institución
• Presupuestal • Financiero • Crédito • Liquidez	• Estratégico o sustantivo • Reputacional o de imagen • Integridad • **Operativo** • Tecnológico • Legal • Administrativo • Servicios • Seguridad • Obra pública • Recursos Humanos

Cuadro 2. Funte: Elaborado por la ASF.

Proceso General de Administración de Riesgos

Acorde con el mandato, características y funcionamiento de los entes gubernamentales, la guía se enfoca a los riesgos no discrecionales, fundamentalmente al riesgo operativo, y se considera como una herramienta de aplicación general.

De forma complementaria, se diseñó el Sistema Automatizado de Administración de Riegos en el Sector Público (SAAR).

El SAAR es una herramienta tecnológica automatizada para gestionar los riesgos institucionales, y es por tanto un componente esencial para implementar la Guía de Autoevaluación de Riesgos en el Sector Público. El SAAR se desarrolló con la finalidad de que la administración de riesgos pueda concebirse y llevarse a cabo de una forma práctica y lógica en instituciones de los tres órdenes de gobierno y Poderes de la Unión.

La figura 1 muestra las principales etapas propuestas para que las instituciones administren de una forma lógica los riesgos a los que se enfrentan:

Objetivos estratégicos	• Establecer de manera precisa los objetivos estratégicos conforme a la normatividad aplicable y en la Administración Pública Federal (APF) con lo dispuesto en el Plan Nacional de Desarrollo (PND) y programa sectorial correspondiente. • Establecer objetivos específicos en cada unidad administrativa y la misión y visión institucional, así como los principios de integridad que la rigen. • Establecer objetivos sobre programas de administración de riesgos.
Identificar	• Identificar los procesos sustantivos, adjetivos y estratégicos, así como los riesgos potenciales que amenazan el logro de los objetivos institucionales. • Identificar posibles eventos en el entorno externo que podrían influir en el logro de los objetivos, por ejemplo, cambios en el marco legal, en la economía, en la política, etcétera).
Evaluar y analizar	• Valorar el posible impacto y probabilidad de ocurrencia que representa la materialización de los riesgos identificados en perjuicio del logro de los objetivos institucionales. • Priorizar los riesgos en términos de mayor a menor impacto y frecuencia para definir las acciones a corto y mediano plazo para su mitigación.
Responder	• Determinar un plan de acción para mitigar, principalmente, los riesgos evaluados con alto impacto y probabilidad de ocurrencia (analizar diferentes opciones para determinar la más adecuada en función de las implicaciones, y características institucionales). • Definir fechas de implementación del plan y sus responsables.
Controlar, monitorear y comunicar	• Seguimiento del avance de las actividades establecidas en el plan de acción y determinar la efectividad en la gestión del riesgo. • Establecer, eliminar o actualizar controles respecto de su efectividad en la mitigación de los riesgos. • Informar al Órgano de Gobierno, Titular y otras instancias de control y vigilancia.

Figura 1. Fuente: Elaborada por la ASF.

La administración de riesgos, ayuda a los mandos superiores, medios y operativos de las instituciones del sector público a tener control sobre aquellos eventos que, en caso de materializarse, puedan afectar el desarrollo y funcionamiento de los procesos para alcanzar los objetivos que persigue la institución.

Dada la pluralidad y particularidad de cada una de las instituciones del sector público, por ejemplo, respecto de las funciones que desempeñan, estructura organizacional, manejo presupuestario, contacto ciudadano y compromiso con la sociedad, es necesario identificar las áreas, procesos o actividades más vulnerables a la ocurrencia de riesgos que atenten contra el logro de sus objetivos.

Las instituciones del sector público, deben contar con un proceso de adiministración de riesgos tendiente a darles un manejo adecuado, con el fin de lograr en términos de eficiencia, eficacia y economía el cumplimiento de sus objetivos y estar preparados para enfrentar cualquier contingencia.

Cabe señalar, que esta guía apunta a fortalecer los sistemas 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 precisa y planeada de la gestión, proporcionando bases para el desempeño adecuado de actividades de control.

La administración de riesgos se lleva a cabo mediante el diseño de un programa destinado para tal objetivo, el cual, debe contener los procedimientos y formas de identificar, evaluar y analizar, responder, controlar, supervisar y comunicar los riesgos institucionales.

La ASF y los demás miembros del Sistema Nacional de Fiscalización tenemos la firme convicción de

que el proceso de fiscalización, rendición de cuentas y combate a la corrupción se fortalecen en la medida en que los programas de gestión de riesgos contribuyen favorablemente al cumplimiento eficaz y eficiente de los objetivos y metas de los planes, programas y proyectos relevantes; propician la generación de información confiable y oportuna; transparentan la administración y control de los recursos públicos; facilitan que las atribuciones se ejerzan dentro del marco legal y normativo aplicable, y protejan los bienes públicos contra el desperdicio y uso inadecuado.

Para implantar un programa de administración de riesgos exitoso se necesita incluir conceptos e ideas integradas en dicho programa, e involucrar a todos los niveles de la institución, con el objetivo de identificar los riesgos que podrian afectar potencialemente sus logros y proporcionar una seguridad razonable del cumplimiento de los objetivos estratégicos.

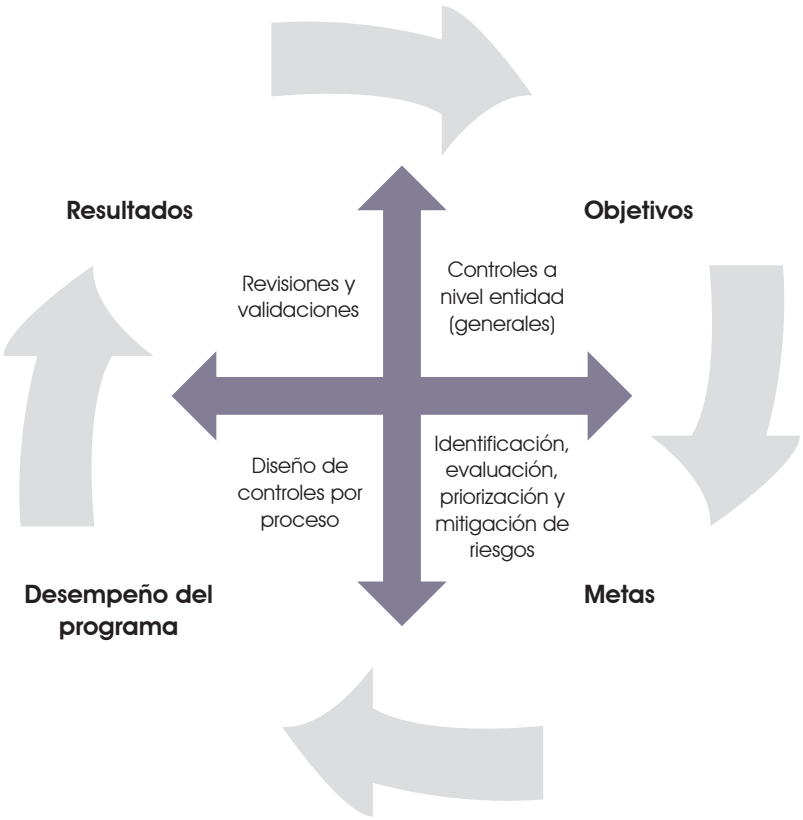

Figura 2. Fuente: Elaborada por la ASF.

La figura anterior muestra la interacción del proceso de la administración de riesgos con la estrategia institucional, al iniciar con la definición de los objetivos estratégicos. Estos últimos requieren la implantación de controles generales que deben observarse por todos los miembros de la institución, por ejemplo el establecimiento formal de una política de integridad, código de ética, código de conducta, etcétera.

Posteriormente, es necesario identificar, evaluar, analizar, responder, controlar, supervisar y comunicar los riesgos que amenazan el logro de los objetivos. La comprensión del entorno institucional tanto interno como externo facilita esta etapa del proceso de administración de riesgos.

El diseño, implantación y medición de la eficacia de los controles a nivel proceso es el siguiente paso para dar respuesta a los riesgos identificados. Es importante señalar que esta actividad es responsabilidad principal de los dueños de los procesos operativos y, en un corto plazo podrá llevarse a cabo mediante la Guía de Autoevaluación de Controles correspondiente que pondrá a disposición del sector público el SNF.

Objetivo

Desarrollar una Guía de Administración de Riesgos que permita a las instituciones del sector público gestionar los riesgos a los que se encuentran expuestos sus procesos sustantivos y adjetivos relevantes, mediante la identificación, evaluación, análisis, respuesta, control, supervisión y comunicación adecuada de esos posibles eventos, con la finalidad de asegurar de forma razonable que se lograrán los objetivos institucionales en términos de eficacia, eficiencia y economía en un marco de transparencia y rendición de cuentas.

Alcance

La guía proporciona directrices para establecer y mantener un marco técnico para la administración general de riesgos, mismo que puede adoptarse por cualquier institución del sector público.

Esta guía se basa principalmente en los cinco componentes del Marco de Control Interno COSO 2013, no obstante, derivado del estudio y análisis de diversos documentos especializados en la materia, resulta compatible con otros modelos o estándares de Control Interno internacionales, que se describen en el siguiente apartado.

1 Sistemas de Control Interno

En el orden internacional, existen diversas asociaciones profesionales especializadas que han emitido documentos y recomendaciones para establecer programas de administración de riesgos, con el propósito de impulsar el logro de los objetivos de los planes, programas y proyectos estratégicos de las organizaciones, sean del sector público o privado. Destacan como modelos de control, por su uso extendido y su probada eficacia, los siguientes: COSO en los Estados Unidos de América, COCO en Canadá, Cadbury y Turnbull en el Reino Unido, ACC en Australia y MECI en Colombia.

El modelo internacional de control integral COSO, emitido por *The Committee of Sponsoring Organizations of the Treadway Commission*[1] se diseñó para apoyar a la alta dirección a tener un mejor control de su organización. En específico, provee un estándar para establecer y evaluar el sistema de control interno. Asimismo, incluye la identificación de riesgos provocados por factores internos y externos asociados con el cambio organizacional. Actualmente es el modelo de control interno de mayor aceptación a nivel mundial.

El modelo canadiense COCO, el cual fue emitido por el Criteria Control Board, ayuda a perfeccionar los procesos de toma de decisiones mediante una mejor comprensión del control del riesgo por parte de la dirección, con base en las teorías de comportamiento. Plantea que los integrantes de la organización deben asumir normas y políticas dadas. Además señala que todas las actividades de la organización deben obedecer a un propósito.

El Informe Cadbury fue publicado en el Reino Unido en diciembre de 1992 por The Committe on the Financial Aspects of Corporate Governance, y la Bolsa de Comercio de Londres lo adoptó como un modelo básico y necesario para las compañías inscritas. Incluye normas que se consideran de práctica aconsejable para los estados financieros; responsabilidades que les competen a los directores y administradores para revisar e informar a los accionistas y otras partes interesadas; composición, rol y desempeño de los comités de auditoría; responsabilidades de directores y administradores en el control, el alcance y el valor de la auditoría, y el establecimiento de los puntos de contacto entre accionistas, directores y auditores.

1 Comité de Organizaciones Patrocinadoras de la Comisión Treadway, integrada por la Asociación Americana de Contabilidad (AAA), el Instituto Americano de Contadores Públicos Certificados (AICPA), los Ejecutivos de Finanzas Internacionales (FEI), el Instituto de Contadores Administrativos (IMA) y por el Instituto de Auditores Internos (IIA), por sus siglas en inglés.

El modelo Turnbull fue diseñado por el Institute of Chartered Accountants of England and Wales. Permite a las instituciones contar con un sistema de control interno que gestiona riesgos operacionales, financieros y legales a los cuales está expuesta. Simultáneamente, ofrece herramientas para garantizar la fiabilidad de los informes financieros y asegurar el cumplimiento de la normativa aplicable a la organización.

El modelo australiano ACC (Australian Control Criteria), da importancia a los empleados y otros grupos de interés para que asuman un nivel apropiado de compromiso en el logro de los propósitos y objetivos en términos de eficiencia y eficacia, legalidad y legitimidad.

El Modelo Estándar de Control Interno (MECI), el cual fue desarrollado en Colombia, tiene por objeto fortalecer el control interno con base en la ética pública, el fortalecimiento del proceso de información y comunicación, la generación de información confiable y oportuna y la promoción de la transparencia en las instituciones.

2 Componentes del marco de control interno COSO 2013

De acuerdo con este modelo, "el control interno es un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos de las operaciones, de los informes y del cumplimiento". Este proceso se encuentra conformado por cinco componentes:

Ambiente de Control
Evaluación de Riesgos
Actividades de Control
Información y Comunicación
Supervisión

Es importante mencionar que, en lo pertinente, el modelo COSO fue el referente para elaborar, tanto la Guía para las Normas de Control Interno del Sector Público emitida en 2001 por la Organización Internacional de las Entidades Fiscalizadoras Superiores (INTOSAI, por sus siglas en inglés) como el "Acuerdo por el que se emiten las Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación General en Materia de Control Interno", emitido en 2010 por la Secretaría de la Función Pública.

La presente guía se enfoca específicamente al componente de evaluación de riesgos; sin embargo, debe señalarse, que los cinco componentes deben existir, funcionar e interactuar entre sí. A continuación se presenta un esquema de la estructura que debe guardar un sistema de control interno y se describen cada uno de sus componentes:

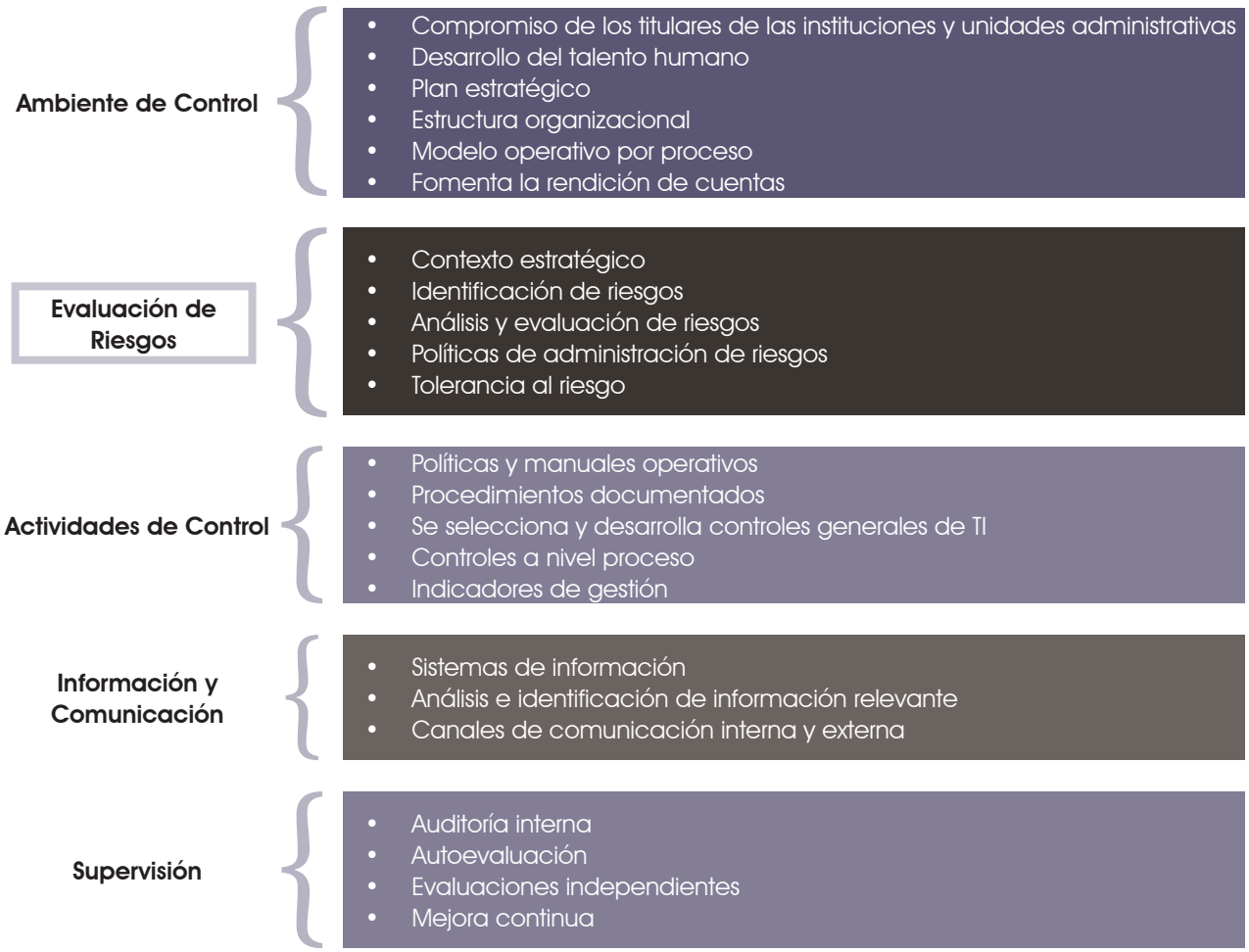

Figura 3. Fuente: Elaborada por la ASF.

2.1 Ambiente de Control

Este componente, comprende la integridad, los valores éticos y la conducta institucional en la organización, es decir, los parámetros que permiten a los titulares y a los órganos de gobierno de los entes gubernamentales llevar a cabo sus responsabilidades de supervisión; determinar la estructura orgánica y la asignación de autoridad y responsabilidad; administrar los recursos humanos a fin de asegurar la atracción, desarrollo y retención de personal competente, y el rigor en torno a medidas de desempeño, estímulos y recompensas para fomentar la rendición de cuentas y la mejora del desempeño.

2.2 Evaluación de Riesgos

Este componente consiste en el proceso para identificar los riesgos a los que están expuestas las instituciones en el desarrollo de sus actividades y analizar los distintos factores, internos y externos, que pueden provocarlos, con la finalidad de definir las estrategias que permitan administrarlos y, por lo tanto, contribuir razonablemente al logro de los objetivos, metas y programas.

Para la administración de riesgos, es fundamental que el Titular de la institución y los mandos superiores de las diversas unidades administrativas promuevan y respalden la cultura de administración de riesgos, mediante mensajes claros que involucren como responsables a todos los servidores públicos en su ámbito de responsabilidad, al buscar la participación

activa de los diferentes niveles de autoridad en la gestión de riesgos.

El riesgo está presente en todas las operaciones de cualquier institución del sector público y se materializa mediante eventos adversos que detonan en pérdidas directas o indirectas, costos por daño reputacional o de imagen, ineficiencia de procesos internos, deficiencia en la administración de personas, y anomalías en sistemas automatizados, entre otras consecuencias inesperadas.

La administración del riesgo operacional se distingue de otros tipos de riesgos, debido a que comprende cualquier limitación, amenaza o problema intrínseco de todas las actividades y procesos inherentes a las operaciones de los entes gubernamentales que, a través de diversos mecanismos de sistemas de mejora de control interno y de prevención del riesgo, busca proteger y fortalecer el patrimonio de las instituciones ante posibles desviaciones o pérdidas económicas por la exposición al riesgo que se tiene. En este sentido, es fundamental que la institución desarrolle una efectiva administración de riesgos que le permita enfrentar o evitar pérdidas económicas, eficientar las operaciones, generar información financiera y no financiera y cumplir con el marco legal y normativo aplicable.

Para el sector público mexicano, el desarrollo del concepto del riesgo puede considerarse como actual e innovador. Para conducir a las instituciones del sector público a cumplir con un estándar internacional de administración de riesgos, la presente guía observa las mejores prácticas establecidas en diferentes documentos como COSO 2013 y COSO ERM, los cuales están enfocados principalmente en la identificación de los objetivos de procesos, los riesgos implícitos a éstos y su cuantificación y, el registro histórico de los materializados.

La guía incluye la identificación de riesgos, su clasificación y la determinación de la probabilidad e impacto de manera cualitativa para definir los controles e indicadores correspondientes que permitan mitigar y supervisar tales riesgos. Para ello, se desarrollan e implementan programas de administración de riesgos, que tienen como fin asegurar la existencia de mecanismos de control, principalmente en los procesos más vulnerables a su ocurrencia.

Las actividades desarrolladas para la administración del riesgo, son un complemento estratégico dentro de la gestión integral de riesgos en las instituciones. Trabajar en sinergia asegura que se identifiquen los riesgos y se definan las respuestas para su mitigación y otras acciones de vigilancia de su comportamiento, según las mejores prácticas internacionales.

2.3 Actividades de Control

Este componente comprende las medidas establecidas en las políticas y manuales de procedimientos para asegurar que la administración pueda mitigar los riesgos que afectan el cumplimiento y logro de los objetivos institucionales. Las actividades de control se llevan a cabo en todos los niveles y procesos de la institución, y en un entorno tecnológico, mediante controles preventivos o detectivos que en su naturaleza pueden abarcar una amplia gama de actividades manuales o automatizadas, tales como autorizaciones y aprobaciones, conciliaciones, evaluaciones de desempeño, etcétera.

2.4 Información y Comunicación

La información es necesaria para que las instituciones lleven a cabo las responsabilidades de control interno en apoyo al logro de sus objetivos. La comunicación se genera tanto interna como externamente; proporciona a la organización la información necesaria para llevar a cabo el control diario, y permite al personal comprender las responsabilidades del control interno y su importancia para el logro de los objetivos institucionales.

2.5 Supervisión

Busca asegurar que los controles operen como se requiere y que sean modificados apropiadamente de acuerdo con los cambios en las condiciones de cada institución a fin de, cumplir con oportunidad y eficiencia las metas y objetivos previstos en sus respectivos programas, conforme a lo dispuesto en la normativa aplicable.

3 Metodología de Administración de Riesgos

Las instituciones del sector público deben cumplir su misión, mediante los objetivos institucionales, los cuales se desarrollan a partir del diseño y ejecución de los diferentes planes, programas y proyectos. El cumplimiento de los objetivos, puede verse afectado por la existencia de riesgos, razón por la cual se hace necesario contar con acciones específicas para administrarlos dentro de la institución. El adecuado manejo de los riesgos beneficia el desarrollo de la institución.

3.1 Principios básicos para una adecuada Administración de Riesgos

Compromiso: Para el éxito de la administración de riesgos, es indispensable el compromiso del Titular de la institución y los mandos superiores de cada unidad administrativa para promover una cultura de identificación y prevención de riesgos, así como definir políticas relacionadas con la administración de riesgos.

Conformación del equipo: Es importante que la institución cuente con un equipo responsable de la implementación del proceso de administración de riesgos, el cual cuente con un canal de comunicación directo con el Titular y mandos superiores de las unidades administrativas. Es recomendable que los integrantes de este equipo cuenten con conocimientos sobre la institución y sobre control interno, administración de riesgos e integridad en el sector público; con el fin de que se facilite la identificación, evaluación, análisis, respuesta, control, supervisión y comunicación de los riesgos; para construir posteriormente un mapa de riesgos institucionales.

Capacitación sobre la guía: Una vez que se cuenta con el equipo responsable del proceso de administración de riesgos, debe capacitarse a sus integrantes en la instrumentación del presente documento.

La figura 4 muestra de manera sintetizada el marco general de administración de riesgos en el sector público:

Marco General de Administración de Riesgos en el Sector Público

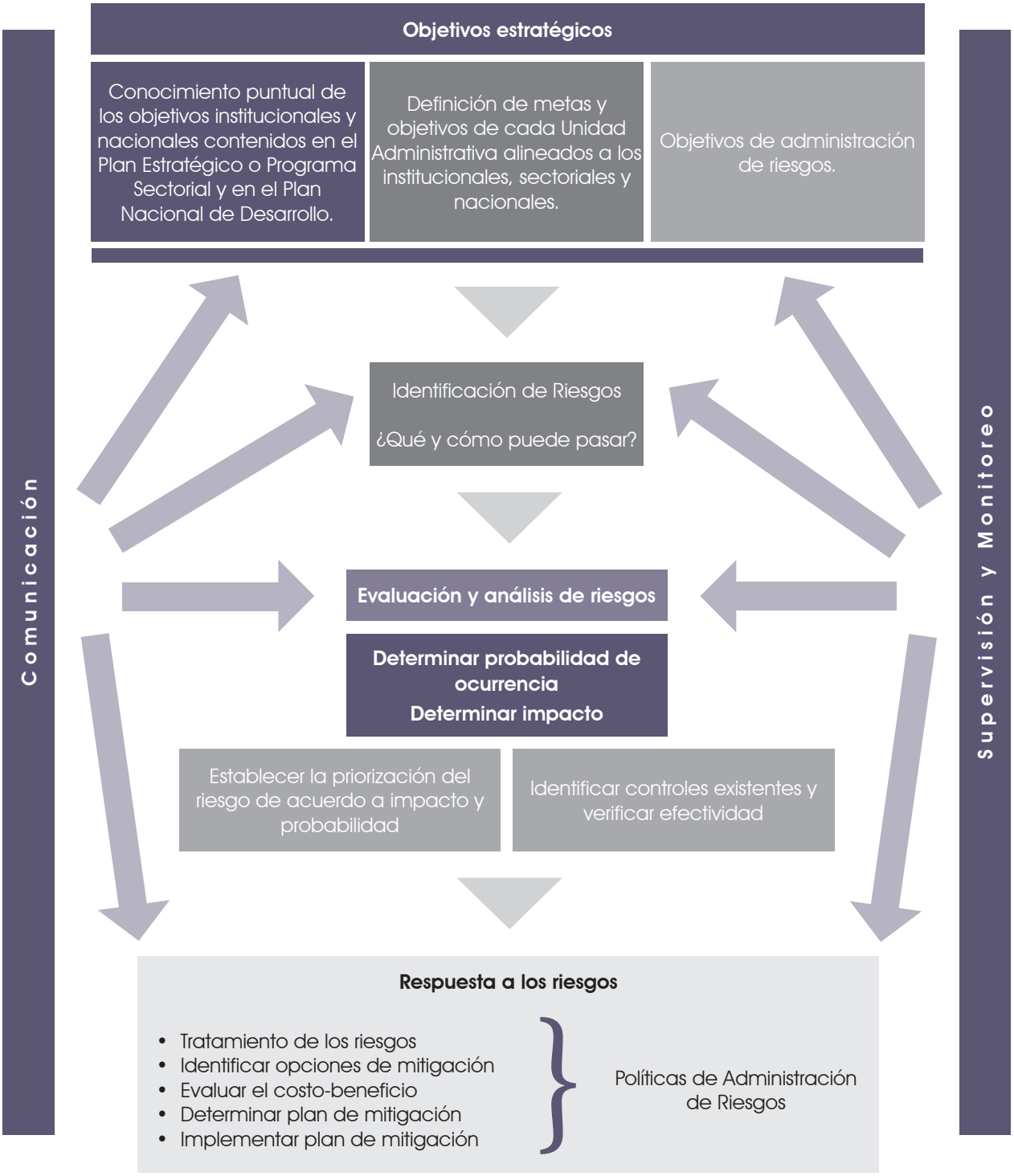

Figura 4. Fuente: Elaborada por la ASF.

3.2 Identificar objetivos estratégicos

Los objetivos estratégicos deben guiar a la organización para el logro de su misión y visión. A partir de éstos se establecen los objetivos operativos, de información y de cumplimiento, así como las metas especificas para las diferentes unidades administrativas.

Las diversas alternativas para alcanzar el cumplimiento de los objetivos estratégicos, involucran identificar los riesgos asociados al considerar sus implicaciones y determinar hasta qué punto la institución puede aceptar determinado riesgo.

Establecer y vigilar los niveles de tolerancia al riesgo proporciona mayor confianza en que los riesgos que enfrentan los objetivos permanecen en un nivel de riesgo aceptado, y a su vez, provee una mayor seguridad de que los resultados esperados serán obtenidos.

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 institución, así como las metas y objetivos estratégicos de la misma. Para lograr lo anterior, se recomienda que dichos servidores públicos revisen:

- Documentos básicos como el Plan Estratégico Institucional, Programa Sectorial y Plan Nacional de Desarrollo, con el propósito de conocer la misión, visión, valores y directrices generales de la institución.
- La estructura orgánica de la institución, así como las atribuciones en el ámbito de su competencia, (reglamento o manual organizacional).
- La alineación de las metas y objetivos particulares de cada unidad administrativa con las metas y objetivos estratégicos.

Para establecer un programa de administración de riesgos es fundamental que los servidores públicos de los diferentes puestos que integran la institución tengan conocimientos referentes a la estrategia institucional. Dicho programa debe atenderse de manera sistémica; es decir, no debe funcionar de manera aislada, sino integral. Esto puede lograrse mediante comunicados y mensajes del Titular de la institución y los altos mandos de las unidades administrativas al resto del personal, quienes indiquen la importancia de la identificación y control de los riesgos.

Como se ha mencionado, el proceso de administración de riesgos considera identificar los factores internos y externos que generan los riesgos contrarios al logro de los objetivos estratégicos.

El análisis de los factores externos se lleva a cabo a partir del conocimiento de situaciones del entorno de la institución, tanto de carácter social, económico, cultural, de orden público, político, legal o tecnológicos. En contraste, el estudio de los factores internos parte del entendimiento actual de la institución, principalmente del componente ambiente de control, estructura organizacional, modelo operativo, cumplimiento de planes y programas, sistema de información, documentación de políticas y procedimientos y recursos financieros, entre los más relevantes.

Para llevar a cabo estos análisis es necesario emplear herramientas como: entrevistas, cuestionarios y lluvia de ideas con servidores públicos de diferentes niveles jerárquicos expertos en el funcionamiento de los procesos de la institución, incluyendo titulares de las unidades administrativas. También es importante llevar a cabo indagaciones con personas ajenas a la institución; desarrollar diagramas de flujo para ubicar posibles riesgos en los procesos; 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 institución.

Asimismo, deben considerarse los registros históricos de riesgos materializados o cercanos a materializarse, opiniones de especialistas y expertos, informes de evaluaciones de años anteriores e indicadores generados en la institución. A continuación se muestran algunos ejemplos de factores internos y externos:

Factores internos	Factores externos
Personal: El perfil de los servidores públicos, la salud laboral, seguridad en el trabajo, ambiente de trabajo, relaciones laborales, diversidad y discriminación; podría detonar riesgos significativos para la institución.	**Cambios en el marco legal:** Podría implicar un riesgo para la institución, debido a que no se encuentra preparada para atender u observar el cumplimiento de nuevos requerientos (Ejemplo: Ley de Contabilidad Gubernamental).
Tecnologías de Información: Confidencialidad de la información, integridad de la información, privacidad de los datos. Indisponibilidad de los sistemas, caída de telecomunicaciones, etcétera; son algunos ejemplos de riesgos detonados en los sistemas institucionales.	**Medioambientales:** Pandemia, terremoto, inundación, incendio, inestabilidad social, etcétera; los factores medioamabientales son factores que detonan riesgos críticos de continuidad de la operación en las instituciones.
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 institución.	

Cuadro 3. Fuente: Elaborado por la ASF.

3.3 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.

En este apartado es necesario diferenciar entre las causas y los efectos de un riesgo. Aunque no siempre es fácil delimitar la frontera entre ambas, las causas definen el origen del riesgo y permiten identificar la esencia de lo que se considera como riesgo y su clasificación (categoría), 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:
Causa: Falta de segregación de funciones. Un servidor público del área de adquisiciones tiene facultades para solicitar, tramitar y autorizar una compra de materiales.
Riesgo potencial: Corrupción. Que un servidor público compre materiales de oficina inecesarios y además los sustraiga, para posteriormente obtener un beneficio personal.
Impacto: Recursos. Pérdida económica para la institución.

Figura 5. Fuente: Elaborada por la ASF.

3.4 Identificación de riesgos

Consiste en determinar cuáles son los tipos de riesgo existentes y cuál es su influencia en las actividades de la institución. Resulta incuestionable que sin una identificación de riesgos apropiada es muy difícil alcanzar una gestión exitosa. Para ello es clave el conocimiento de las fuentes de riesgo, realizar un inventario de riesgos y analizar las causas de los eventos que los generan. La identificación, representa una de las actividades clave dentro del proceso de administración de riesgos, debido a que dicha actividad debe iniciar con reconocer los procesos y subprocesos por los cuales se cumplen los objetivos institucionales.

Es importante llevar a cabo una clasificación de los diferentes tipos de riesgos que existen en los siguientes grupos: estratégico, financiero, operativo, legal, tecnológico, a la integridad y a la reputación o imagen.

Desde el punto de vista técnico – metodológico, para el estudio de las causales, según el enfoque de administración de riesgos, destaca la dinámica de los sistemas automatizados que permiten pasar de un enfoque cualitativo a uno más cuantitativo y establecer un sistema integral basado en retroalimentación el cual facilita el control de los procesos y la minimización de riesgos materializados.

Como se ha mencionado antes, la identificación de riesgos es el primer procedimiento de la administración de riesgos e incluye la revisión de factores tanto internos como externos que podrian influir en la adecuada implementación de la estrategia y logro de objetivos. Además, los responsables de la implementación de proceso de administración de riesgos, con el apoyo de los mandos superiores, identifican las relaciones entre los riesgos y su clasificación para crear un lenguaje de riesgos común en la institución.

3.4.1 Técnicas para la identificación de riesgos

A continuación se muestran y describen de manera breve las técnicas para identificar riesgos en las instituciones:

Figura 6. Fuente: Elaborada por la ASF.

1. **Talleres de autoevaluación:** Consisten en reuniones de servidores públicos de diferentes niveles jeráquicos que dempeñen actividades clave en la institución; con el objetivo de identificar los riesgos, analizar y evaluar su posible impacto en el cumplimiento de los objetivos y proponer acciones para su mitigación.

2. **Mapeo de procesos:** Esta técnica consiste en revisar el diagrama del proceso operativo e identificar los puntos críticos que podrían implicar un riesgo. Para efectuarla es necesario que se encuentren documentados todos los procesos de la institución.

3. **Análisis de entorno:** Consiste en la revisión de cambios en el marco legal, entorno económico o cualquier factor externo que podría amenazar el cumplimiento de los objetivos.

4. **Lluvia de ideas:** Se trata de una técnica grupal en la que participan actores de diferentes niveles jerárquicos para generar ideas relacionadas con los riesgos, causas, eventos o impactos que pueden poner en peligro el logro de los objetivos.

5. **Entrevistas:** Éstas consisten en realizar una serie de preguntas relacionadas con los eventos que amenazan el logro de los objetivos. Se aplican a servidores públicos de diferentes niveles jerárquicos de una o varias unidades administrativas.

6. **El análisis de indicadores de gestión, de desempeño o de riesgos:** Deberán establecerse con anterioridad y evaluar sus desviaciones, es decir, que su comportamiento está por encima o debajo del rango normal, esto debe analizarse para determinar si esa desviación se debe a algun riesgo materializado o su comportamiento anormal tiene alguna explicación diferente a un riesgo.

7. **Cuestionarios:** Consisten en una serie de preguntas enfocadas a detectar las preocupaciones de los servidores públicos de mandos superiores, medios u operativos sobre riesgos que se perciben en las actividades que desempeñan.

8. **Análisis comparativo:** Comprenden el análisis entre instituciones que desarrollan actividades similares, con el fin de identificar riesgos que podrían afectar a la institución.

9. **Registros de riesgos materializados:** Consiste en bases de datos con los riesgos materializados en el pasado en la institución. Estos registros deben contener la descripción del evento, fecha, monto de pérdida, si se llevó a cabo alguna recuperación y qué control se estableció para mitigar el riesgo y que cierta situación vuelva a repetirse.

Una de las herramientas que funciona de manera más adecuada para la identificación de riesgos son los talleres; sin embargo, las otras técnicas pueden utilizarse como complemento, de tal forma que mediante la combinación de varias herramientas se logre una cobertura más amplia en la identificación de riesgos.

Durante el proceso de identificación de riesgos es preciso clasificarlos en primera instancia de acuerdo con su tipología, con el fin de comprender las causas e impacto que dichos riesgos pueden tener en caso de materializarse.

3.4.2 Clasificación de riesgos

El proceso de identificación incluye la clasficación de los riesgos considerando por lo menos las siguientes categorías:

Estratégico: Se asocia a los asuntos relacionados con la misión y el cumplimiento de los objetivos estratégicos.

Financiero: Se relaciona con los recursos económicos de la institución, principalmente de la eficiencia y transparencia en el manejo de los recursos.

Operativo: Este rubro considera los riesgos relacionados con fallas en los procesos, en los sistemas o en la estructura de la institución.

Legal: Afecta la capacidad de la institución para dar cumplimiento a la legislación y obligaciones contractuales.

Tecnológico: Se relaciona con la capacidad de la institución para que las herramientas tecnológicas soporten el logro de los objetivos estratégicos.

A la integridad: Son aquellas situaciones o eventos que, en caso de materializarse, impactarían en mayor o menor medida al entorno de valores y principios éticos de la institución.

A la reputación o imagen: Se refleja en un impacto de la materialización de cualquier tipo de riesgo, pues podría implicar presencia en cualquiera de las categorías de riesgo descritas anteriormente.

3.4.3 Desarrollo de talleres de trabajo para la identificación de riesgos

1. Designar a un responsable para moderar los talleres, este servidor público deberá contar con conocimientos necesarios sobre los procesos y las actividades que se van a analizar; asimismo, deberá contar con conocimientos sobre control interno y administración de riesgos. Es recomendable que el Titular de la institución designe al moderador.

2. Conformar el equipo multidisciplinario y con servidores públicos de diferentes niveles jerárquicos. Lo ideal es formar equipos de entre 20 y 30 servidores públicos.

3. Analizar el contexto en el que se encuentra la institución, identificar los objetivos institucionales, analizar el plan estratégico, la estructura organizacional, y demás elementos referentes a los propósitos fundamentales de la institución.

4. Es importante realizar, previo al taller, una relación de los procesos sustantivos, adjetivos y estratégicos de la institución; para ubicar que procesos deberán estar en alcance del análisis de riesgos; a continuación se muestra una lista general de los procesos con mayor exposición a riesgos:

Proceso	Riesgo
Procesos sustantivos	Errores humanos Fallas de sistemas institucionales Fallas de procesos
Procesos adjetivos	Errores humanos Fallas de sistemas institucionales Fallas de procesos Falta de cumplimiento al marco legal
Recursos materiales (compras generales, contratación de proveedores, licitaciones, etc.)	Riesgos de integridad (soborno, nepotismo, desviación de recursos)
Recursos humanos (nómina, bonos, incentivos, contratación de personal, etc.)	Riesgos de integridad (soborno, nepotismo, desviación de recursos)
Recursos financieros (tesorería, inversiones, contabilidad, finanzas, presupuestos, impuestos, gastos, etc.)	Riesgos de integridad (soborno, nepotismo, desviación de recursos)
Tecnologías de información (sistemas instituciones, telecomunicaciones, red, servidores, bases de datos, etc.)	Integridad de la información Disponibilidad de los sistemas institucionales Virus Caída de sistemas institucionales

Cuadro 4. Fuente: Elaborado por la ASF.

5. Una vez que se ha determinado que procesos son los más vulnerables, deberá revisarse cada una de sus actividades para determinar en conjunto a que riesgos específicamente se encuentran expuestos, esto se lleva a cabo con la ayuda del moderador. Para identificar los riesgos es necesario realizar la pregunta clave, ¿qué puede suceder?

6. El responsable deberá registrar todos los riesgos que sean mencionados por los integrantes del grupo de trabajo, para posteriormente análizar cuales de ellos deben considerarse, ya que debe darse prioridad a los riesgos más significativos.

La identificación de riesgos es una actividad crítica dentro de la administración de riesgos, ya que en caso de tener inconsistencias en esta etapa, el desarrollo de los procedimientos subsecuentes puede tener repercusiones. Dicha actividad se realiza a partir del entendimiento de los procesos y subprocesos y detección de los posibles eventos que pueden afectar el cumplimiento de los propósitos estratégicos.

Para puntualizar las fallas o problemas se debe partir de las actividades intrínsecas establecidas por las instituciones en los procesos sustantivos, adjetivos y estratégicos (por lo que es indispensable contar con un mapeo completo de los procesos de la institución). A continuación se muestra la matriz en la cual se lleva el registro de los riesgos identificados:

Identificación del riesgo											
Número de riesgo	Proceso	Objetivo del proceso	Tipo de proceso	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Clasificación del riesgo	Causa del riesgo	Tipo de factor	Consecuencia del riesgo	Área del riesgo

Cuadro 5. Fuente: Elaborado por la ASF[2].

La identificación de los riesgos debe ser acorde con su causa primaria; es decir, aquellas que los originan dentro del proceso o subproceso, en especial debe cuidarse separar eventos transferidos por otras áreas o procesos.

La matriz de identificación de riesgos permite que las instituciones lleven el registro de los riesgos detectados, para contar con un inventario de los mismos, al determinar el objetivo, proceso o plan que puede verse afectado por un determinado riesgo, así como las causas y el impacto posible.

Durante el desarrollo de la etapa de identificación de riesgos, las instituciones deben dar prioridad a los procesos críticos y los riesgos más relevantes.

Es importante señalar que, como se ha mencionado anteriormente, de forma complementaria a esta guía se diseñó el SAAR para llevar a cabo el registro de los riesgos, el cual permitirá a las instituciones del sector público llevar una adecuada administración de riesgos. Dicha herramienta incluye un instructivo para el usuario, que apoya el uso y aprovechamiento de los recursos institucionales.

3.5 Evaluación de riesgos

La evaluación es la etapa subsecuente a la identificación del proceso de administración de riesgos, en la cual se valora la probabilidad de ocurrencia del riesgo y el impacto que puede producir en caso de que se materialice.

La evaluación de riesgos se lleva a cabo con técnicas cualitativas que consisten en valorar la probabilidad desde una perspectiva de juicio de expertos, quienes conocen de manera muy precisa las actividades, los procesos y el entorno en el cual se desempeña la

2 Matriz incluida en el Sistema Automatizado de Administración de Riesgos.

institución. Existen también técnicas cuantitativas para evaluar riesgos, las cuales, consisten en determinar el valor de un riesgo mediante modelos estadísticos y calcular la pérdida esperada por materialización de riesgos; para utilizar estas técnicas, se necesita contar con información suficiente en tiempo y calidad, es decir, que la institución tenga registros de riesgos materializados de por lo menos los últimos cinco años.

- La **probabilidad** de ocurrencia se valora con base en la frecuencia; es decir, cuántas veces podría ocurrir el riesgo; considerando los factores internos y externos.

- El **impacto** se valora tomando en cuenta las consecuencias que pueden ocasionar a la institución en caso de que el riesgo se materialice.

A continuación se muestra las escalas para la evaluación de riesgos en probabilidad e impacto:
En el grado de impacto, debe considerarse el valor 10 de mayor jerarquía y 1 de menor. El orden los factores o criterios puede variar, dependiendo del mandato, naturaleza y circunstancias de cada institución.

Escala de evaluación de la probabilidad de ocurrencia del riesgo

Valor	Categoría	Probabilidad
10	**Recurrente**	Muy alta, se tiene plena seguridad que éste se materialice, tiende a estar entre 90% y 100%.
9		
8	**Muy probable**	Alta, se tiene entre 75% a 95% de seguridad que éste se materialice.
7		
6	**Poco probable**	Media, se tiene entre 51% a 74% de seguridad que éste se materialice.
5		
4	**Inusual**	Baja, se tiene entre 25% a 50% de seguridad que éste se materialice.
3		
2	**Rara**	Muy baja, se tiene entre 1% a 25% de seguridad que éste se materialice.
1		

Cuadro 6. Fuente: Elaborado por la ASF.

Escala de evaluación del impacto en caso de materializarse el riesgo

Valor	Categoría	Impacto
10	**Catastrófico**	Influye directamente en el cumplimiento de la misión, visión y objetivos de la institución; asimismo puede implicar pérdida patrimonial o daño de la imagen, dejando además sin funciones total o parcialmente por un periodo importante de tiempo, afectando los programas o servicios que entrega la institución.
9		
8	**Grave**	Podría dañar de manera significativa el patrimonio institucional, daño a la imagen o logro de los objetivos estratégicos. Asimismo se necesita un periodo de tiempo considerable para restablecer la operación o corregir los daños.
7		
6	**Moderado**	Causaría una pérdida importante en el patrimonio o un daño en la imagen institucional.
5		
4	**Bajo**	No afecta el cumplimiento de los objetivos estratégicos y que en caso de materializarse podría causar daños al patrimonio o imagen, que se puede corregir en poco tiempo.
3		
2	**Menor**	Podría tener efectos muy pequeños en la institución.
1		

Cuadro 7. Fuente: Elaborado por la ASF.

La evaluación del riesgo debe estimar la probabilidad de ocurrencia de un riesgo y el impacto que puede causar en la institución; dicha estimación se realiza utilizando las dos escalas anteriores.

Es importante que esta evaluación se lleve a cabo cada 3 meses, con la finalidad de mantener actualizados los riesgos de acuerdo con el entorno interno y externo de la institución.

A continuación se muestra un ejemplo de la matriz de evaluación de riesgos:

Evaluación de riesgos			
Probabilidad	**Impacto**	**Valor del Riesgo**	**Prioridad del Riesgo**
1	3	2.2	Bajo
7	6	6.4	Alto
10	10	10	Muy alto
2	9	6.2	Alto
6	3	4.2	Medio
4	7	5.8	Alto

Cuadro 8. Fuente: Elaborado por la ASF.

3.6 Priorización de los riesgos

Una vez realizada la valoración de la probabilidad e impacto, es necesario priorizar los riesgos, este proceso lo realiza de manera automática el Sistema Automátizado de Adiministración de Riesgos y permite determinar cuáles riesgos requieren un tratamiento inmediato, de acuerdo con el siguiente mapa de calor (Ver figura 9) que ubica cada riesgo identificado en la zona del mapa que le corresponda de acuerdo con su evaluación; de esta forma la institución está en posibilidades de establecer sus niveles de tolerancia a los riesgos.

La escala para priorizar riesgos se muestra a continuación y determina la gravedad del riesgo de acuerdo con la probabilidad e impacto determinados al momento de la evaluación.

Escala para priorizar los riesgos

Riesgo bajo 1-2.4	**Zona de riesgo tolerable.** Determinar si los riesgos ubicados en esta zona se aceptan, previenen o mitigan.
Riesgo moderado 2.5-4.9	**Zona de riesgo moderado.** Determinar si las medidas de prevención y vigilancia para los riesgos ubicados en esta zona, se comparten o transfieren para mitigarlos de manera adecuada.
Riesgo alto 5-7.5	**Zona de riesgo alto.** Determinar si las medidas para mitigar los riesgos ubicados en esta zona, se comparten o transfieren para gestionarlos de manera adecuada.
Riesgo grave 7.6-10	**Zona de riesgo significativo.** Tomar las medidas necesarias para mitigar los riesgos que se encuentran en esta zona, es recomendable establecer un plan para tales fines.

Cuadro 9. Fuente: Elaborado por la ASF.

3 Matriz incluida en el Sistema Automatizado de Administración de Riesgos.

3.7 Evaluación de controles

Una vez que se han identificado, evaluado y priorizado los riesgos; es necesario revisar las actividades de control que existen para mitigarlos; asimismo, es importante evaluar qué tan efectivos son los controles que se encuentran establecidos tanto en su operatividad como en su diseño; esta actividad es clave, ya que la existencia de controles inadecuados o inefectivos manifiestan una gestión de riesgos nula.

A continuación se muestra la matriz de valoración básica de los controles asociados a los riesgos identificados y evaluados, ya que en el corto plazo, se emitirá la Guía de Autoevaluación de Controles.

CONTROLES									
Número de control	Nombre de control	Tipo de control	Frecuencia de Ejecución	Área responsable del control	Evidencia de la ejecución	Evidencia del control	Efectividad del control	Diseño del control	¿Existe riesgo residual?

Cuadro 10. Fuente: Elaborado por la ASF[4].

3.7.1 Establecimiento de controles para el éxito

El establecimiento de estrategias de administración de riesgos basadas en las mejores prácticas se diseñan con base en una gestión directiva que emplea una filosofía de respaldo total sobre el control. Las características generales que debe considerar un efectivo sistema de administración de riesgos, son las siguientes:

1. Enfocarse en la necesidad de generar o aumentar el rendimiento.
2. Contribuir a que los titulares trabajen de forma efectiva.
3. Compararse con instituciones similares es crucial para una gestión exitosa.
4. Trabajar apropiadamente y dar apoyo a los colegas en todos los niveles de responsabilidad.
5. Establecer indicadores de gestión del desempeño significativos y útiles.
6. Identificar y enfrentar los problemas de forma eficiente.
7. Consultar a los auditores, y que ellos cuenten con las competencias necesarias.
8. Entender el riesgo y considerarlo como propio en las distintas unidades administrativas.
9. Buscar objetivos desafiantes y que beneficien a la organización.
10. Entender y mejorar continuamente el sistema de administración de riesgos.

Una filosofía de control de acuerdo con las mejores prácticas conduce a un marco moderno de aplicación práctica, el cual, refleja resultados exitosos para la organización en su conjunto, al promoverse a lo largo de las líneas de: "¿Estamos todos en el control que realmente nos hace exitosos?".

4 Matriz incluida en Sistema Automatizado de Administración de Riesgos.

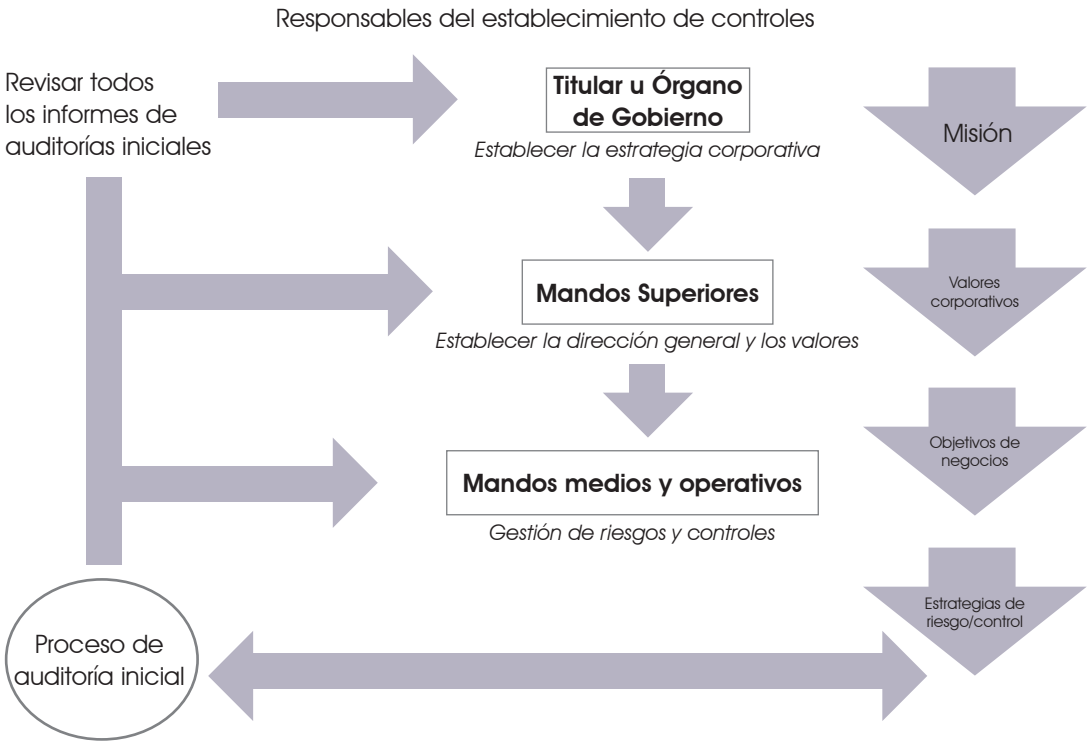

Figura 7. Fuente: Elaborada por la ASF.

El Titular es el responsable principal de establecer una estrategia institucional que respalde el ciclo de administración de riesgos y el sistema de administración de riesgos en su conjunto. Asimismo, debe aplicar un claro sentido de dirección en donde las personas conocen los riesgos que enfrenta su institución y se convierten en responsables del manejo de los riesgos que pueden afectar las metas específicas de las unidades administrativas en las que desarrollan sus actividades y de los objetivos estratégicos que están alineados con la misión institucional.

3.8 Política de respuesta al riesgo

La institución cuenta con una serie de procesos para ejecutar varias operaciones, las cuales consisten en las entradas, el proceso, y las salidas. Mientras los riesgos puedan afectar esa dinámica, tienen que contrarrestarse por controles efectivos.

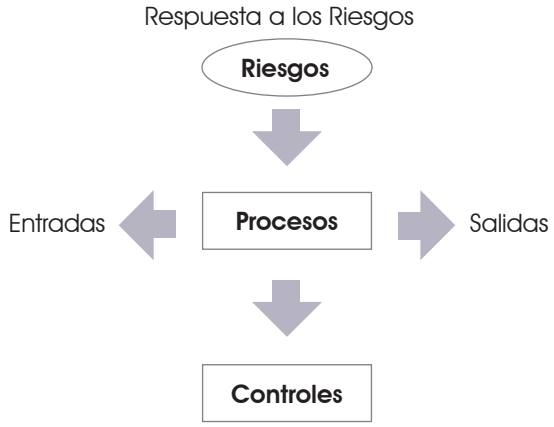

Figura 8. Fuente: Elaborada por la ASF.

Para responder a los riesgos evaluados, la institución analiza y determina las acciones correspondientes que deben emprenderse, considerando el impacto y la probabilidad determinada, con el fin de alinear los riesgos evaluados con el apetito de riesgo, estrategia y objetivos.

La institución debe analizar diversas alternativas para emprender posibles respuestas a los riesgos, incluyendo las que se enfocan a asumirlos, vigilarlos, evitarlos, transferirlos, reducirlos y compartirlos. Es de vital importancia realizar un análisis del beneficio ante el costo en la mitigación de los riesgos para que posteriormente se establezcan políticas de administración de riesgos.

Asumir el riesgo: Una vez analizado el grado de impacto que el riesgo tiene sobre los objetivos estratégicos y que se concluye que no está en condiciones de mitigarlo razonablemente, se decide retenerlo y no ejecutar acción alguna. Esta estrategia deberá usarse sólo

para riesgos de bajo impacto y baja probabilidad de ocurrencia.

Vigilar el riesgo: En este supuesto, debe darse seguimiento periódico al riesgo para determinar su probabilidad de ocurrencia conforme transcurre el tiempo. Si la probabilidad de ocurrencia se incrementa, los responsables de administrar los riesgos deberán actuar de manera inmediata implementando acciones para mitigarlo. Este tipo de estrategias es aplicable para riesgos de alto impacto y baja probabilidad de ocurrencia. Se recomienda crear un plan para mitigarlo sólo si aumenta la probabilidad de ocurrencia.

Evitar el riesgo: Este tipo de respuesta se refiere a eliminar el factor o los factores que están provocando el riesgo; es decir, si una parte del proceso tiene alto riesgo, el segmento completo recibe cambios sustanciales por mejora, rediseño o eliminación, resultado de contratos suficientes y acciones emprendidas; sin embargo, este tipo de estrategia no es recomendable por la naturaleza de las actividades de las instituciones.

Transferir el riesgo: Esta respuesta consiste en trasladar el riesgo mediante la responsabilización de un tercero (tercerización especializada). El tercero debe tener experiencia particular para ejecutar el trabajo sin riesgos o si el riesgo permanece. La responsabilidad será del tercero y asumirá los impactos o perdidas derivadas de su materialización. En la actualidad la estrategia de transferencia de riesgos es una de las más utilizadas; cuenta con tres dimensiones que se detallan a continuación:

- **Protección o cobertura:** Cuando la acción que se realiza para reducir la posibilidad de una pérdida, obliga también a renunciar a la posibilidad de una ganancia.
- **Aseguramiento:** Significa pagar una prima (el precio del seguro) para que en caso de tener pérdidas estas sean asumidas por la aseguradora.
- **Diversificación:** Implica mantener cantidades similares de muchos activos riesgosos en lugar de concentrar toda la inversión en uno sólo producto.

Reducir el riesgo: Esta estrategia aplica cuando un riesgo ha sido identificado y representa una amenaza para el cumplimiento de los objetivos estratégicos, proceso o áreas, por lo que la institución deberá establecer acciones dirigidas a disminuir la probabilidad de ocurrencia (acciones de prevención) y el impacto (acciones de contingencia), tales como medidas específicas de control interno y optimización de procedimientos.

Compartir el Riesgo: Se refiere a distribuir el riesgo y las posibles consecuencias, también puede entenderse como transferencias parciales, en las que el objetivo no es deslindarse completamente, sino segmentarlo y canalizarlo a diferentes unidades administrativas o personas, las cuales se responsabilizarán de la parte del riesgo que les corresponda.

El efecto de adoptar una estrategia o la combinación de éstas, tendrá como resultado un riesgo remanente o residual, el cual debe asumise responsablemente por los titulares de las unidades administrativas de que se trate.

3.8.1 Respuesta al riesgo residual

El riesgo residual es aquel que permanece después de que la institución ha llevado a cabo las actividades para responder a los riesgos; refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la institución para enfrentar el riesgo inherente. Estas acciones pueden incluir las políticas y procedimientos que establezcan límites, autorizaciones y otros protocolos; es decir se ven reflejadas en actividades de control. El siguiente cuadro muestra el tratamiento del riesgo residual.

Respuesta al riesgo residual				
Respuesta al riesgo	Acciones de respuesta	Entregable de acciones	Área responsable de la respuesta	Fecha de entrega

Cuadro 11. Fuente: Elaborado por la ASF[5].

Los niveles y su correspondencia con las zonas que determinan la prioridad y el tipo de respuesta que necesita el riesgo para gestionarlo de manera adecuada, se muestran en el cuadro 9 de la página 23.

3.9 Informe al titular de la institución sobre los riesgos que se detectaron

Posterior a la identificación, evaluación, análisis y priorización de los riesgos, se procederá a informar al Titular de la institución los resultados más relevantes, como se describe a continuación:

- Los resultados se comentarán en reunión con el Titular de la institución.
- Debe presentarse la matriz de identificación de riesgos con el objetivo de determinar las acciones correspondientes para la administración de riesgos.
- Los resultados deberán informarse también al comité de riesgos o su equivalente.

3.10 Matriz general de riesgos

Cada uno de los apartados anteriores, forman parte de la matriz de riesgos y controles; dicha matriz constituye una herramienta de gestión de riesgos, la cual se encuentra automatizada en el SAAR, ésta permite a las instituciones documentar los procesos y objetivos críticos y correlacionarlos con los riesgos que amenazan el logro de los mismos; de esta forma, se determina el nivel de riesgo, control y tipo de respuesta que requiere cada riesgo. A continuación se muestra la matriz de riesgos consolidada:

Matriz de riesgos															
Identificación del riesgo												Evaluación de riesgos			
Número de riesgo	Proceso	Objetivo del proceso	Tipo de proceso	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Clasificación del riesgo	Causa del riesgo	Tipo de factor	Consecuencia del riesgo	Área del riesgo	Probabilidad	Impacto	Valor del riesgo	Prioridad del riesgo
												1	3	2.2	Bajo
												7	6	6.4	Alto
												10	10	10	Muy alto
												2	9	6.2	Alto
												6	3	4.2	Medio
												4	7	5.8	Alto
												3	8	6	Alto
												8	7	7.4	Alto
												6	5	5.4	Alto

Controles										Respuesta al riesgo				
Número de control	Nombre del control	Tipo de control	Frecuencia de ejecución	Área responsable del control	Evidencia de la ejecución	Evidencia del control	Efectividad del control	Diseño del control	¿Existe riesgo residual?	Respuesta al riesgo	Acciones de Respuesta	Entregable de acciones	Área responsable de la respuesta	Fecha de entrega

Cuadro 12. Fuente: Elaborado por la ASF.

3.11 Mapa de riesgos

El mapa permite ubicar qué riesgos tienen mayor grado de frecuencia e impacto; a partir de esto deberá decidirse que respuesta para los riesgos ubicados con niveles altos deben llevarse a cabo.

El SAAR también permite visualizar la ubicación de los riesgos de la forma siguiente:

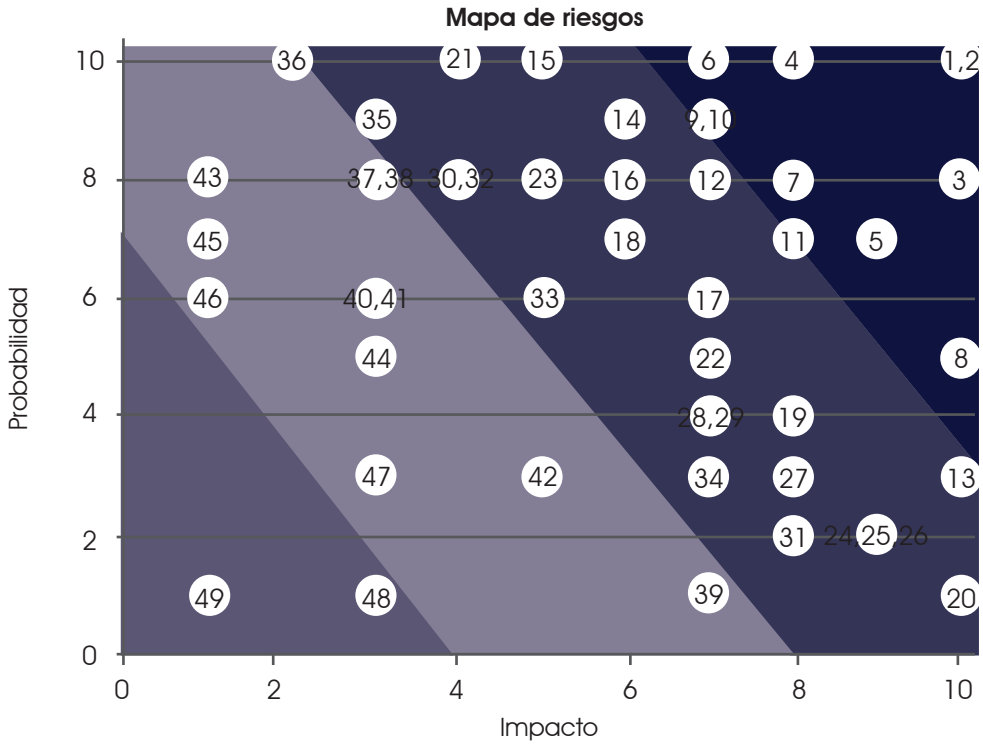

Figura 9. Fuente: Elaborada por la ASF.

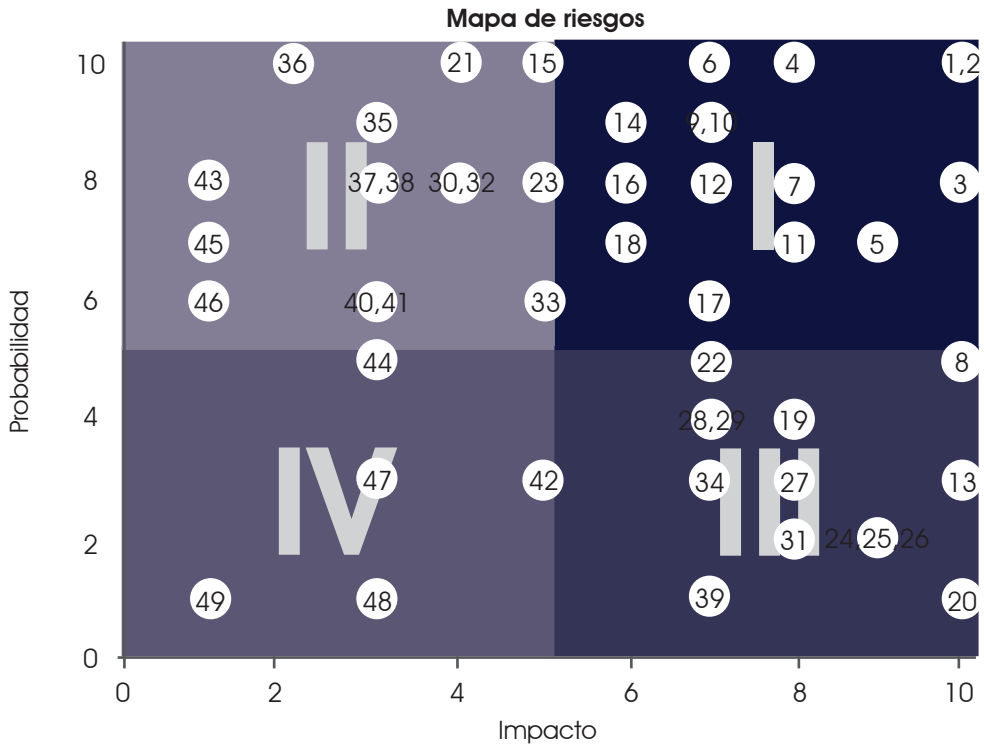

Figura 10. Fuente: Elaborada por la ASF

3.12 Nivel de Tolerancia al riesgo y apetito de riesgo

La tolerancia y el apetito de riesgo son términos muy usados, y que a menudo se utilizan de manera indistinta; sin embargo, existe diferencia entre ambos términos.

El apetito de riesgo de acuerdo con el COSO 2013, es el riesgo que la institución está dispuesta a aceptar en la búsqueda del logro de sus objetivos y metas institucionales.

Por otro lado, la tolerancia al riesgo es el nivel aceptable de variación en los resultados o actuaciones de la institución relacionada con la consecución o logro de los objetivos. La tolerancia al riesgo es la cantidad máxima de un riesgo que una institución puede soportar sin causar graves daños al logro de los propósitos del ente.

Apetito de Riesgo. Es una aprobación de alto nivel de aceptación de un riesgo en el logro de los objetivos. Principales características:

- Establecer el apetito de riesgo a nivel de institución.
- Es posible expresarlo o establecerlo mediante un mapa de calor.

Tolerancia al Riesgo. Es el nivel aceptable de diferencia respecto al logro de los objetivos. 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 (qué nivel de riesgo está dispuesto a aceptar).
- Establecer riesgos que la institución no está dispuesta a aceptar (por ejemplo: en el cumplimiento del marco legal).

3.12.1 Cómo debe establecerse el nivel de tolerancia a los riesgos

1. El Titular propondrá los niveles de tolerancia necesarios para la gestión del riesgo, mismos que someterá al Comité de Riesgos o su equivalente para su aprobación.

2. El Titular revisará los niveles de tolerancia aprobados al menos una vez al año o cuando se requiera, con la finalidad de asegurar que se encuentran en los niveles razonables y cualquier cambio que se requiera se someterá a aprobación del Comité de Riesgos o su equivalente.

3. Una vez aprobados los niveles de tolerancia, serán comunicados a las áreas involucradas.

4. El Titular instruirá realizar la supervisión periódica, ya sea mensual o de acuerdo con la frecuencia establecida en los indicadores, y el comportamiento de los niveles de tolerancia se informará al Comité de Riesgos o su equivalente de manera trimestral por medio del reporte de riesgo emitido.

5. Los responsables de cada riesgo deben supervisar el comportamiento de los niveles de tolerancia mediante indicadores de riesgos establecidos por el Titular y autorizados por el Comité de Riesgos o su equivalente.

6. En caso de que el nivel de riesgo observado exceda el nivel de tolerancia autorizado, los responsables del riesgo, informarán del riesgo al Cómite de Riesgos o su equivalente inmediatamente después de haberla detectado.

4 Plan de Continuidad del Negocio (PCN)

Es un proceso administrativo integrado, transversal a toda la institución, el cual permite mantener alineadas y vigentes todas las iniciativas, estrategias, actores, planes de respuesta y demás componentes de la continuidad del negocio. Su finalidad es responder ante una crisis, incidente o desastre que amenaza la continuidad de las operaciones de la institución.

Estos planes buscan mantener la continuidad de la operaciones en la entrega de los productos o servicios de acuerdo con el mandato institucional antes, durante y después de una interrupción general de cualquier tipo.

4.1 Resiliencia

Es la capacidad de un sistema, expuesto a una amenaza, para resistir, absorber, adaptarse y recuperarse de sus efectos de manera oportuna y eficaz, lo que incluye la preservación y la restauración de sus estructuras y funciones básicas.[6]

La resiliencia como concepto, proviene de la física de los materiales y a manera de ejemplo se puede expresa por medio de las cualidades de un resorte, es decir, qué tanto puede resistir a la presión, doblarse con flexibilidad y recobrar su forma original. La imagen de un resorte que se estira y regresa a su forma original, refleja la resiliencia, que toma el sentido de la capacidad de "resistir a" o de "resurgir de" un choque o una crisis.

La resiliencia de una institución con respecto a los posibles eventos que resulten de una amenaza, se determina por el grado en que la institución cuenta con los recursos necesarios y es capaz de organizarse tanto antes como durante una crisis o un desastre natural, por ejemplo, un terremoto, inundación, incendio, etc. Este concepto incluye a los servidores públicos, procesos sustantivos, adjetivos y estratégicos, tecnología e infraestructura.

El daño reputacional y la interrupción de las operaciones, encabezan la lista de los mayores impactos para las instituciones del sector público. Hoy en día, la continuidad del negocio no sólo se asocia con fenómenos físicos

6 2009 UNISDR Terminología sobre Reducción del Riesgo de Desastres, Pág. 28, Organización de las Naciones Unidas (ONU)

como incendios o fallos tecnológicos, sino que se extiende a un nivel estratégico en el que la reputación y el valor de las instituciones en cuanto a credibilidad y confianza de la ciudadanía, son elementos clave.

Contar con un Plan de Continuidad del Negocio permite a las instituciones garantizar la continuidad de la actividad frente a una crisis, aumentando las posibilidades de supervivencia de la institución.

4.2 Ventajas del PCN

El Plan de Continuidad de Negocio es una herramienta que permite prevenir o evitar los posibles escenarios originados por una situación de crisis, así como minimizar las consecuencias económicas, reputacionales o de responsabilidad civil derivadas de la misma. Ayuda además a reducir los costos asociados a la interrupción o evitar penalizaciones contractuales por incumplimiento de contratos como proveedor de productos o servicios.

4.3 Contenido del PCN

El Plan de Continuidad del Negocio permite anticiparse a la situación de crisis y garantizar el desarrollo normal de la actividad, determinando los riesgos de magnitud suficiente para poder responder ante el peligro de un evento, continuar con el funcionamiento normal de las actividades de la institución y señalando las acciones a adoptar en caso de que algún riesgo se materialice. Asimismo, ayuda a determinar de antemano qué información es crítica y cómo debe salvaguardarse. Estos planes son una herramienta de estabilidad y continuidad que aporta prestigio a las instituciones que los implantan.

4.4 Metodología del PCN

El proyecto se inicia en las operaciones y progresa hasta garantizar su continuidad, los resultados de cada etapa alimentan a la siguiente, con lo que se logra una evolución coherente. A lo largo del desarrollo del proyecto, se cubren los siguientes objetivos.

1.- Obtener una imagen clara y detallada de los procesos sustantivos y adjetivos relevantes de la institución, determinando sus criticidades, interdependencias y riesgos.
2.- Lograr un conocimiento profundo de la plataforma tecnológica.
3.- Determinar las necesidades críticas para permitir un grado de operatividad en línea con los planes estratégicos y metas definidas.
4.- Desarrollar una solución cuya relación costo-beneficio cumpla con los requisitos y las expectativas de la institución.
5.- Prever y documentar las acciones necesarias para restaurar las actividades de la institución.

Diferencias entre PCN Y PRS

El PRCD o Plan de Recuperación en caso de Desastres plantea:

Realizar planes de prevención y recuperación ante los escenarios de desastre con mayor impacto y probabilidad de ocurrencia.

El ámbito del PRCD son los sistemas de información de la organización.

Dentro de los PRCD son críticos los tiempos de pérdida y recuperación de información.

El PCN o Plan de Continuidad del Negocios extiende el alcance:

El PCN tiene como objetivo el mantenimiento de la actividad en la institución, bien mediante la recuperación de los procesos de soporte o mediante la aplicación de procesos de emergencia.

Dentro del PCN es clave el análisis de impacto en las operaciones que toma en cuenta el impacto económico cuando se detenienen las actividades en la institución.

4.5 PCN y Sistema de Gestión de la Seguridad de la Información (SGSI)

- La existencia de un PCN se considera una parte clave en la implantación de un SGSI.

- Una medida básica de seguridad en cualquier organización es la disponibilidad y acceso a la información crítica.

4.5.1 ISO 27001

Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del Sistema de Gestión de la Seguridad de la Información. Tiene su origen en la BS 7799-2:2002 (anulada) y es la norma a la cual se certifican los SGSIs de las organizaciones por auditores externos.

La norma ISO/IEC 27001:2005 pretende adecuarse a diferentes tipos de uso, incluyendo los siguientes:

- Utilizada por las organizaciones para formular los requisitos y objetivos de seguridad;

- Utilizada por las organizaciones como una forma de garantizar que los riesgos de seguridad son gestionados eficazmente;

- Utilizada por las organizaciones para asegurar el cumplimiento con las leyes y reglamentos;

- Utilizada en una organización como un marco de procesos para el establecimiento y gestión de controles que garanticen el cumplimiento de los objetivos específicos de seguridad de una organización;

- Definición de nuevos procesos de gestión de la seguridad de la información;

- Identificación y clarificación de los procesos de gestión de la seguridad de la información existentes;

- Utilizada por la administración de las organizaciones para determinar el estado de las actividades de gestión de la seguridad de la información;

- Utilizada por los auditores internos y externos de las organizaciones para determinar el grado de cumplimiento con las políticas, directrices y normas adoptadas por la organización;

- Utilizada por las organizaciones para proporcionar información relevante acerca de las políticas, directivas, normas y procedimientos de seguridad de la información a los proveedores y otras organizaciones con las que interactúan por razones operativas.

4.5.2 Estrategia de administración de riesgos (nivel de madurez)

Las instituciones del sector público deben establecer un programa de administración de riesgos y una estrategia en cuanto a su comunicación y difusión, ya que cada institución debe asegurar razonablemente que los servidores públicos que forman parte de ésta participen de manera activa en la administración de riesgos.

Las instituciones que tienen menor nivel de madurez en la administración de riesgos se enfrentan a dificultades para identificar riesgos y para definir cómo afectan éstos a la estrategia institucional. Las políticas de riesgo deben ser documentos dinámicos que contengan un mensaje desde el comienzo de la administración de riesgos y ser entendidos, aplicados y reportados.

En la implementación de políticas de riesgos, los entes gubernamentales deben considerar las siguientes cuestiones prácticas que afectan la manera de administrar el riesgo:

- Debe tenerse una administración de riesgos efectiva en toda la institución, al punto de que algunos de los beneficios que percibe el personal sean basados en el logro del plan

estratégico, sin dejar de lado el marco jurídico y legal aplicable.
- La política de riesgos debe ser ratificada por algún comité (preferentemente el de riesgos) y relacionarla con la visión, misión y plan estratégico, incorporando la administración de riesgos como parte de una cultura deseada en el estilo de la gestión de la institución.
- La política de riesgos debe contener datos claros que identifiquen los diferentes tipos de riesgos, incluyendo categorías de riesgos en grupos clave.
- Definir roles y responsabilidades referentes a la administración de riesgos, sobre todo en lo referente a la propiedad, evaluación y seguimiento de los mismos.
- Determinar acciones que deben desarrollarse cuando se presentan los riesgos o surjan fallas en los controles.
- Mantener el entendimiento de las políticas de riesgos entre los servidores públicos con encuestas regulares y entrevistas selectivas.
- Describir los riesgos y controles, y el modo en que los riesgos clave deben registrarse en un sistema de reportes.
- Definir la relación entre la administración de riesgos, el sistema de control y la política de integridad institucional.
- Definir qué es considerado un control clave, e indicar si los riesgos registrados deben ser sujetos a una revisión formal o a una determinada respuesta.
- Puntualizar la relación causa-efecto y la tendencia hacia la gestión de riesgo de la institución mediante un mapa de riesgos institucional.
- Precisar el modo en que el proceso de la administración de riesgos tiene y preserva su calidad, y cómo las decisiones institucionales deben basarse en el análisis de los riesgos.
- Describir el impacto en la reputación, operación, integridad, etc., de la institución en caso de materializarse los riesgos.
- Capacitación continua en temas relacionados con el programa de administración de riesgos, que garantice la existencia de una cultura institucional de administración de riesgos.
- Comunicar los programas, políticas y procesos de administración de riesgos para permear esta conciencia de riesgos en todo el personal de la institución.

El seguimiento y supervisión de los riesgos son parte de la mejora continua, y el Titular debe establecer mecanismos que permitan el seguimiento para valorar el grado de avance y las mejoras necesarias que deben hacerse para reforzar e impulsar la administración de riesgo, hasta lograr una madurez adecuada en el programa de administración de riesgos.

Glosario

Se incluye el siguiente glosario para mayor precisión en las definiciones relacionadas con el proceso de Administración de Riesgos:

Término	Descripción
Acción (es) de mejora	Las actividades determinadas e implantadas por los titulares y demás servidores públicos de las instituciones para fortalecer el Sistema de Control Interno Institucional, así como prevenir, disminuir, administrar y/o eliminar los riesgos que pudieran obstaculizar el cumplimiento de objetivos y metas.
Administración de riesgos	El proceso sistemático que deben de realizar las instituciones para evaluar y dar seguimiento al comportamiento de los riesgos a que están expuestas en el desarrollo de sus actividades, mediante el análisis de los distintos factores que pueden provocarlos, con la finalidad de definir las estrategias y acciones que permitan controlarlos y asegurar el logro de los objetivos y metas de una manera razonable.

Análisis de Costo-Beneficio	Una herramienta de Administración de Riesgos usada para tomar decisiones sobre las técnicas propuestas por el grupo para la administración de los 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 al costo.
Área (s) de oportunidad	La situación favorable en el entorno institucional, bajo la forma de hechos, tendencias, cambios o nuevas necesidades que se pueden aprovechar.
Autocontrol	La implantación que realizan los titulares de las instituciones, de los mecanismos, acciones y prácticas de supervisión o evaluación de cada sistema, actividad o proceso; ejecutado de manera automática por los sistemas informáticos, o de manera manual por los servidores públicos; y que permite identificar, evitar y, en su caso, corregir con oportunidad los riesgos o condiciones que limiten, impidan o hagan ineficiente el logro de objetivos.
Causa	Son los medios, circunstancias y agentes precursores de los riesgos.
Comité y/o COCODI	El Comité de Control y Desempeño Institucional, órgano colegiado que contribuye al cumplimiento de los objetivos y metas institucionales; a impulsar el establecimiento y actualización del Sistema de Control Interno, y al análisis y seguimiento para la detección y administración de riesgos, conforme a lo dispuesto en el Título Cuarto de las presentes Disposiciones en Materia de Control Interno.
Control correctivo	El mecanismo específico de control que opera en la etapa final de un proceso, el cual permite identificar y corregir o subsanar en algún grado, omisiones o desviaciones.
Control detectivo	El mecanismo específico de control que opera en el momento en que los eventos o transacciones están ocurriendo, e identifican las omisiones o desviaciones antes de que concluya un proceso determinado.
Control Interno	El proceso que tiene como fin proporcionar un grado de seguridad razonable en la consecución de los objetivos de la institución.
Control preventivo	El mecanismo específico de control que tiene el propósito de anticiparse a la posibilidad de que ocurran situaciones no deseadas o inesperadas que pudieran afectar al logro de los objetivos y metas.
Costo	Se entiende por costo las erogaciones, directas e indirectas en que incurre la institución en la producción, prestación de un servicio o manejo de un riesgo, por ejemplo, adquirir una póliza de fidelidad para transferir el riesgo de fraude por un costo.
Debilidad de Control Interno	La insuficiencia, deficiencia o inexistencia identificada en el Sistema de Control Interno Institucional mediante la supervisión, verificación y evaluación interna y/o de los órganos de fiscalización, que pueden evitar que se aprovechen las oportunidades y/u ocasionar que los riesgos se materialicen.

Debilidad de Control Interno de mayor importancia	La insuficiencia, deficiencia o inexistencia identificada que obstaculizan o impiden el logro de los objetivos y metas institucionales, o motivan la existencia de un riesgo que eventualmente genere un daño al erario público federal.
Evaluación de riesgos	Determinar el impacto y la probabilidad del riesgo. Dependiendo de la información disponible pueden emplearse desde modelos de simulación, hasta técnicas colaborativas.
Dependencias	Las secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, conforme a lo dispuesto en la Ley Orgánica de la Administración Pública Federal.
Disposiciones	Las disposiciones en materia de control interno.
Economía	Los términos y condiciones bajo los cuales se adquieren recursos, en cantidad y calidad apropiada y al menor costo posible para realizar una actividad determinada, con la calidad requerida.
Eficacia	El cumplimiento de los objetivos y metas establecidos, en lugar, tiempo, calidad y cantidad.
Eficiencia	El logro de objetivos y metas programadas con la menor cantidad de recursos.
Encuesta de autoevaluación por nivel de Control Interno	La herramienta que aplican los servidores públicos de una institución, en el ámbito de su competencia por nivel de control interno (estratégico, directivo y operativo) para conocer los avances en el establecimiento y actualización de los elementos del Sistema de Control Interno Institucional.
Entidades	Los organismos públicos descentralizados, empresas de participación estatal mayoritaria y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales son considerados instituciones del Sector Público Paraestatal.
Estrategia para manejar el riesgo	Actividades determinadas y específicas que elige la institución para evitar o prevenir, reducir, dispersar, transferir y asumir riesgos.
Evaluación del Sistema de Control Interno	El proceso mediante el cual se determina el grado de eficacia y de eficiencia con que se cumplen los elementos de control del Sistema de Control Interno Institucional en sus tres niveles: Estratégico, Directivo y Operativo, para asegurar el cumplimiento de los objetivos del Control Interno institucional.
Factor de riesgo	La circunstancia o situación interna y/o externa que aumenta la probabilidad de que un riesgo se materialice.
Grado de madurez de la Administración de Riesgos Institucional	El número de controles suficientes establecidos con relación al número de riesgos inventariados.
Grado de madurez del Sistema de Control Interno Institucional	La medición del nivel de aplicación y estandarización de los elementos de Control Interno que integran los componentes del sistema en un contexto de mejores prácticas, que se obtendrá con la implementación de las encuestas.

Identificación de riesgos	Establecer la estructura del riesgo; fuentes o factores, internos o externos, generadores de riesgos; puede hacerse a cualquier nivel: toda la institución por áreas, por procesos, incluso, bajo el viejo paradigma, por funciones; desde el nivel estratégico hasta el más humilde operativo.
Impacto o efecto	Las consecuencias negativas que se generarían en la institución, en el supuesto de materializarse el riesgo.
Indicador	Es la valoración de una o más variables que informa sobre una situación y soporta la toma de decisiones, es un criterio de medición y de evaluación cuantitativa o cualitativa.
Informe Anual	Informe Anual del estado que Guarda el Sistema de Control Interno Institucional.
Intitución o Intituciones	Dependencias e instituciones del Sector Público Federal, Estatal o Municipal, según corresponda, así como en los Órganos Constitucionales Autónomos, en su caso.
Manual	El Manual Administrativo de Aplicación General en Materia de Control Interno a que se refiere el artículo cuarto del Acuerdo en el que se emiten las Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación General en Materia de Control Interno, el cual integra diversos procesos asociados con el Control Interno.
Mapas de riesgos institucional	La representación gráfica de uno o más riesgos que permite vincular la probabilidad de ocurrencia y su impacto en forma clara y objetiva.
Matriz de Administración de Riesgos Institucional	El tablero de control que refleja el diagnóstico general de los riesgos para contar con un panorama de los mismos e identificar áreas de oportunidad en la institución.
Modelo Estándar de Control Interno	La herramienta para el establecimiento y actualización del Sistema de Control Interno en las instituciones del sector público.
Nivel de riesgo (determinación del)	Es el resultado de correlacionar el impacto y la posibilidad, con los controles internos existentes.
Nivel (es) de Control Interno	La implementación y actualización de los elementos de Control Interno que integran las cinco Normas Generales de Control Interno, que realizan los servidores públicos adscritos a las instituciones de acuerdo al ámbito de su competencia y nivel jerárquico y se clasifican en: Estratégico, Directivo y Operativo, en apego a los numerales 14 y 16 del Acuerdo por el que se emiten las Disposiciones en Materia de Control Interno.
Normas Generales de Control Interno	La implementación y actualización de los elementos de Control Interno que integran los cinco componentes del Control Interno que realizan los servidores públicos adscritos a las instituciones, de acuerdo al ámbito de su competencia y nivel jerárquico.
OIC	El órgano interno de control de la dependencia o institución.
Oportunidad	La generación y entrega de la información y documentación en el tiempo requerido para su uso.
Órgano de gobierno	El cuerpo colegiado de la administración de las instituciones, de conformidad con los artículos 17 y 18 de la Ley Federal de las Entidades Paraestatales y 2 de su Reglamento.

Órgano (s) fiscalizador (es)	La instancia facultada para realizar la revisión, supervisión, evaluación, control y seguimiento del ejercicio de los recursos públicos de acuerdo a las disposiciones legales, reglamentarias y normas administrativas, así como del cumplimiento de los objetivos contenidos en planes y programas institucionales, con el propósito de detectar desviaciones, prevenir, corregir, mejorar y/o sancionar.
Plan de contingencia	Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la institución.
Plan y programa de acción	Programa de manejo del riesgo que contiene las técnicas de administración del riesgo orientadas a prevenir, evitar, reducir, dispersar, transferir o asumir riesgos.
Planeación estratégica	El ejercicio periódico que facilita la identificación de fortalezas, oportunidades, debilidades y amenazas, a través del cual se integra un programa de trabajo que permite establecer las palancas o acciones estratégicas o prioritarias, en virtud de que son las que derivan el mayor impacto en resultados, satisfacción y confianza de la sociedad.
Probabilidad o posibilidad	Una medida (expresada como porcentaje o razón) para estimar la posibilidad de que ocurra un incidente o evento. Contando con registros, puede estimarse a partir de su frecuencia histórica mediante modelos estadísticos de mayor o menor complejidad.
PTAR	El Programa de Trabajo de Administración de Riesgos.
PTCI	El Programa de Trabajo de Control Interno.
Responsables	Son los servidores públicos encargadas de monitorear un riesgo y dar seguimiento a planes de acción propuestos.
Retroalimentación	Información sistemática sobre los resultados alcanzados en la ejecución de un plan, que sirven para actualizar el nivel de riesgos deseado.
Riesgo	El evento adverso e incierto (externo o interno) que derivado de la combinación de su probabilidad de ocurrencia y el posible impacto pudiera obstaculizar o impedir el logro de los objetivos y metas institucionales.
Riesgo inherente	Es aquel al que se enfrenta una institución en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
Riesgo residual	Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.
Seguimiento	Recolección regular y sistemática sobre la ejecución del plan, que sirven para actualizar y mejorar la exposición a riesgos.
Seguridad razonable	El escenario en el que la posibilidad de materialización del riesgo disminuye, y la posibilidad de lograr los objetivos se incrementa.

Sistema de Control Interno Institucional	El conjunto de procesos, mecanismos y elementos organizados y relacionados que interactúan entre sí, y que se aplican de manera específica por una institución a nivel de planeación, organización, ejecución, dirección, información y seguimiento de sus procesos de gestión, para dar certidumbre a la toma de decisiones y conducirla con una seguridad razonable al logro de sus objetivos y metas en un ambiente ético, de calidad, mejora continua, eficiencia y de cumplimiento de la ley.
Sistema de información	El conjunto de procedimientos ordenados que, al ser ejecutados, proporcionan información para apoyar la toma de decisiones y el control de la institución.
Técnicas cualitativas	Las técnicas cualitativas se utilizan cuando los riesgos no se prestan a la cuantificación o cuando no están disponibles datos suficientes y creíbles para una evaluación cuantitativa o la obtención y análisis de ellos no resulte eficaz por su coste.
Técnicas cuantitativas	Las técnicas cuantitativas pueden utilizarse cuando existe la suficiente información para estimar la probabilidad o el impacto del riesgo empleando mediciones de intervalo o de razón. Los métodos cuantitativos incluyen técnicas probabilísticas, no probabilísticas y de análisis comparativo. Una consideración importante en la evaluación cuantitativa es la disponibilidad de información precisa, ya sea de fuentes internas o externas, y uno de los retos que plantea el uso de estas técnicas es de obtener datos válidos.
TIC´s	Las Tecnologías de la Información y Comunicaciones.
Unidades administrativas	Las comprendidas en el reglamento interior, estatuto orgánico y/o estructura orgánica básica de una institución, responsable de ejercer la asignación presupuestaria correspondiente.
Valoración del riesgo	Fase en la administración de riesgos, diagnóstico que consta de la identificación, análisis y determinación del nivel de riesgo.

Énfasis sobre la implementación de esta Guía

Para la adopción de esta guía, las instituciones deben incorporar todas las etapas generales en ella descritas, a fin de preservar la cohesión en la atención integral y sistémica de los riesgos institucionales. La omisión de alguna de dichas etapas o partes de las mismas puede propiciar que el proceso de administración de riesgos esté incompleto y debilitado.

Si la institución considera, con base en el criterio prudencial del responsable de la administración de riesgos, que su sistema para operar este proceso cuenta con el nivel de madurez establecido en la presente guía o lo supera, puede optar por continuar con la operación del mismo.

En tal caso, es necesario que el servidor público antes señalado informe formalmente al Titular, al Órgano de Gobierno, al Comité de Control y Desempeño Institucional, a los Comités de Auditoría, de Control Interno o de Riesgos, según corresponda, las razones que justifiquen lo anterior, así como la manera en que se atienden los propósitos de la autoevaluación de riesgos con los procedimientos existentes.

Al documentar y comunicar esta situación, la institución estará en condiciones de aclarar la manera en que sus prácticas reales son consistentes con los principios contenidos en las mejores prácticas; de cómo contribuyen a la mejora de los procesos de autoevaluación de riesgos y promueven la consecución de los objetivos estratégicos, así como la salvaguarda de los recursos públicos.

ASF Auditoría Superior de la Federación

CÁMARA DE DIPUTADOS