



*Al servicio
de las personas
y las naciones*

Protocolo de análisis de riesgos

Proyecto “Apoyando el cumplimiento de los Objetivos de Desarrollo Sostenible en México por medio de prácticas de gobierno abierto, participación ciudadana y el fortalecimiento de la transparencia” implementado por el Programa de las Naciones Unidas para el Desarrollo (PNUD) en conjunto con la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), en apoyo al proyecto “Fortalecimiento y acompañamiento del Programa de Integridad” de la Secretaría de la Función Pública.

Este estudio/reporte fue posible gracias al apoyo del pueblo de los Estados Unidos, a través de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID). El contenido de este estudio/reporte es responsabilidad del proyecto Apoyando el cumplimiento de los Objetivos de Desarrollo Sostenible en México por medio de prácticas de gobierno abierto, participación ciudadana y el fortalecimiento de la transparencia y no necesariamente refleja el punto de vista de USAID o del gobierno de los Estados Unidos; ni del Programa de las Naciones Unidas para el Desarrollo, de su Junta Directiva, ni de sus Estados Miembros.

Este Programa de Formación fue posible gracias al apoyo del pueblo de los Estados Unidos, a través de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID). El contenido de este Programa de Formación es responsabilidad del proyecto Apoyando el cumplimiento de los Objetivos de Desarrollo Sostenible en México por medio de prácticas de gobierno abierto, participación ciudadana y el fortalecimiento de la transparencia y no necesariamente refleja el punto de vista de USAID o del gobierno de los Estados Unidos; ni del Programa de las Naciones Unidas para el Desarrollo, de su Junta Directiva, ni de sus Estados Miembros.

Ciudad de México, abril de 2018

**PROGRAMA DE LAS NACIONES UNIDAS PARA EL DESARROLLO EN MÉXICO
(PNUD)**

Antonio Molpeceres
Coordinador Residente del Sistema de Naciones Unidas
y Representante Residente del Programa de las Naciones Unidas para el Desarrollo
en México

Katyna Argueta
Directora de País

Javier González
Director del Programa de Gobernabilidad Democrática

Vania Pérez
Coordinadora del Proyecto de Integridad y Fortalecimiento de la Transparencia

Óscar Cárdenas
Administrador del Proyecto

Maite García de Alba
Especialista en Política Social

Lorena Arredondo
Especialista en Monitoreo y Evaluación

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO EN MÉXICO

Antonino De Leo
Representante UNODC, México

Lorena De La Barrera
Coordinadora de Proyectos Anticorrupción, Integridad
y Prevención del Delito Financiero

Laura Bertipaglia
Especialista Junior en Prevención de la Corrupción en el Sector Privado

Melisa Moreno Martínez
Auxiliar Logístico

Prólogo

La Convención de las Naciones Unidas Contra la Corrupción (UNCAC, 2003), por sus siglas en inglés, a la que México está adherida, llama a cada Estado Parte a promover y fortalecer las medidas para prevenir y combatir la corrupción en los sectores público y privado, bajo un enfoque novedoso donde la corresponsabilidad de todos los actores de la sociedad es clave para fomentar la cultura de la integridad y buenas prácticas comerciales.

En ese marco, el Congreso de la Unión aprobó en mayo de 2015 las reformas constitucionales que crean el Sistema Nacional Anticorrupción. Un año después, en julio de 2016, se publicaron las leyes secundarias, entre ellas la Ley General de Responsabilidades Administrativas (LGRA), que establece las obligaciones de los servidores públicos y de las personas morales en la prevención y combate de la corrupción.

Como una herramienta de apoyo a las empresas para cumplir con la nueva legislación, la Secretaría de la Función Pública (SFP) elaboró y presentó a su vez, en junio de 2017, un Modelo de Programa de Integridad Empresarial, que establece los lineamientos generales para que el sector privado diseñe e implemente políticas anticorrupción.

Para promover el cumplimiento de una Política de Integridad Empresarial, en el marco del Proyecto “Apoyando el cumplimiento de los Objetivos de Desarrollo Sostenible en México por medio de prácticas de gobierno abierto, participación ciudadana y el fortalecimiento de la transparencia” el Programa de las Naciones Unidas para el Desarrollo (PNUD) en conjunto con la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), se apoyó el proyecto “Fortalecimiento y acompañamiento del Programa de Integridad” de la Secretaría de la Función Pública”. El objetivo de la iniciativa es consolidar la política de integridad empresarial en México con el acompañamiento de pequeñas y medianas empresas mexicanas en la implementación del primer componente del Programa para la Integridad de la SFP, representado por el Modelo de Programa de Integridad empresarial, a través del acercamiento de herramientas para la prevención de la corrupción y la consolidación de una política de integridad en el sector privado.

Para cumplir con este objetivo, se han diseñado seis productos dirigidos a pequeñas y medianas empresas que tienen relación comercial con el sector público, principalmente, con el objetivo de que desarrollen e implementen una Política de Integridad Empresarial. Estos productos se realizaron en colaboración con cámaras empresariales y cuerpos colegiados de profesionistas con quienes se conformó el Grupo de Trabajo Empresarial (GTE), encargado de participar en el diseño e implementación de dichos productos.

Los miembros que integraron el Grupo de Trabajo Empresarial son:

1. Alliance for Integrity
2. Asociación Mexicana de Industrias Innovadoras de Dispositivos Médicos, AMID

3. Asociación Nacional de Abogados de Empresa, Colegio de Abogados, A.C., ANADE
4. ASPEN Institute
5. Cámara Internacional de Comercio, ICC México
6. Cámara Mexicana de la Industria de la Construcción, CMIC
7. Cámara Nacional de Empresas de Consultoría, CNEC
8. Cámara Nacional de la Industria del Vestido, CANAIVE
9. Cámara Nacional de la Industria Farmacéutica, CANIFARMA
10. Cámara Nacional de Manufacturas Eléctricas, CANAME
11. Cámara Suizo-Mexicana de Comercio e Industria
12. Colegio de Contadores Públicos de México, CCPM
13. Confederación de Cámaras Industriales, CONCAMIN
14. Confederación Patronal de la República Mexicana, COPARMEX
15. Consejo Coordinador Empresarial, CCE
16. Consejo de Ética y Transparencia de la Industria Farmacéutica, CETIFARMA
17. Corporación Mexicana de Asesores en Derecho S.C., COMAD, S.C
18. Ilustre y Nacional Colegio de Abogados de México, A.C.
19. Instituto Mexicano de Contadores Públicos, IMCP
20. OCA LAW FIRM / Instituto Mexicano de Ejecutivos de Finanzas, IMEF
21. Secretaría de la Función Pública, SFP
22. The Global Compact, Red Pacto Mundial México
23. Unión de Instituciones Financieras Mexicanas, UNIFIMEX

Un Programa de Integridad Empresarial se fundamenta en dos pilares: la promoción de la cultura de la integridad y una metodología de gestión de riesgos de corrupción. Por ello, los cuatro productos elaborados en el marco del Proyecto pretenden ser materiales de apoyo para promover en las empresas la cultura de la integridad en los negocios en tanto que representan una propuesta metodológica para gestionar los riesgos de corrupción:

1. Glosario de términos hacia la integridad corporativa: se explican y refieren los principales términos relacionados a la lucha contra la corrupción, la integridad, el cumplimiento y las nuevas especificaciones legales.
2. Documento de Mapeo y Reporte de Buenas Prácticas para la Prevención y el Combate a la Corrupción y Promoción de la Integridad en Pequeñas, Medianas y Grandes Empresas en México 2017-2018: que reúne las buenas prácticas aplicadas por los integrantes del Grupo de Trabajo Empresarial (GTE) y contenidas en diversos documentos proporcionados por los mismos.
3. Código de Conducta Modelo: el Código de Conducta Modelo establece los principios mínimos para actuar en una empresa y representa una guía para desarrollar herramientas que promuevan la cultura de la integridad empresarial.

4. Manual de Implementación del Código de Conducta: el Manual de Implementación contiene la metodología a seguir para implementar un Código de Conducta. Se caracteriza por ejemplos y preguntas guías que las Pymes pueden tomar en cuenta para la correcta implementación del Código.

5. Protocolo para el Análisis de Riesgos: el Protocolo para el Análisis de Riesgos representa una guía enfocada a la evaluación y gestión de riesgos de corrupción contenidos en los artículos 66 a 72 de la Ley General de Responsabilidades Administrativas (LGRA), así como los elementos de control establecidos en el artículo 25 del mismo ordenamiento.

6. Herramienta de Autodiagnóstico: la Herramienta de Autodiagnóstico sirve como mecanismo de verificación de cumplimiento del Programa de Integridad. Es un instrumento para evaluar el riesgo de cumplimiento de la normatividad aplicable a empresas de cualquier sector y condición o ubicación geográfica, e incluso cámaras, gremios y asociaciones. La herramienta está ejemplificada con riesgos de corrupción de los artículos 66 a 72, que pueden ser mitigados con los controles establecidos en el artículo 25, todos ellos de la Ley General de Responsabilidades Administrativas (LGRA).

Los documentos modelo representan asimismo el “qué” y el “cómo” implementar un programa de integridad. El Código de Conducta establece qué lineamientos deben seguir los colaboradores de una empresa, el Manual es una guía para implementar políticas y procedimientos para hacer cumplir esos lineamientos y el documento de Mapeo de Buenas Prácticas otorga ejemplos de diversas políticas y procedimientos probados con éxito en diversas latitudes. Por su parte, el Protocolo de Riesgos explica qué pasos debe seguir una empresa para monitorear y mitigar los riesgos y la Herramienta de Autodiagnóstico propone cómo ejecutarlos. Por esta razón, se invita a revisar y utilizar de forma relacionada los seis documentos referidos, como una caja de herramienta para empezar a diseñar e implementar un Programa de Integridad Empresarial.

Finalmente, hay que destacar que, estos productos, al hacerse del dominio público, especialmente entre las Pymes tendrán un alto impacto en la construcción de una cultura del cumplimiento y legalidad para avanzar juntos hacia la integridad. La recomendación es que las cámaras empresariales y asociaciones de profesionistas, en un ejercicio de corresponsabilidad, retomen estos materiales, los adecuen en caso de ser necesario, y lideren los esfuerzos para materializar y garantizar el cumplimiento de las obligaciones derivadas del nuevo Sistema Nacional Anticorrupción.

Prólogo	4
Introducción. Cultura de la prevención	9
I. Gestión de riesgos	12
1.1. ¿Qué es un riesgo?	12
1.2 Tipos de riesgos	13
1.3 Riesgo de cumplimiento	14
II. Etapas de la gestión de riesgos de cumplimiento	15
2.1 Identificar riesgos	15
2.2 Priorizar riesgos	16
2.3 Evaluar riesgos	16
2.3.1 Riesgo inherente	16
2.3.2 Evaluar controles	17
2.3.3 Riesgo residual	17
2.4 Monitoreo	18
2.5 Planes de acción	19
2.6 Revisión (<i>testing</i>) y auditoría	19
III. Comunicación	21
IV. Preguntas y respuestas	22
V. Algunos estándares internacionales de gestión de riesgo	23
VI. Comentarios de metodología	24
VII. Anexos	25

Cultura de la prevención

Como lo refiere la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés) en su *Resource Guide on State Measures for Strengthening Corporate Integrity*,¹ es frecuente decir que, para las empresas, un gramo de prevención vale más que un kilo de cura, lo que solo se logra con un programa interno efectivo para prevenir y detectar violaciones a la ley o a estándares éticos. Estos programas se denominan de “cumplimiento” o “prevención”.

Para asegurar que la implementación de un Programa de Cumplimiento sea efectiva y eficiente, debe aplicarse una metodología de Gestión de Riesgos, que permita la identificación, priorización, evaluación, medición y monitoreo de riesgos y posteriormente elaborar planes de acción. Dicha metodología es aplicable a cualquier organización pública o privada, incluyendo las de corte empresarial. Sus componentes básicos han sido probados en el mundo de los negocios por más de veinte años con resultados positivos.

El presente *Protocolo de análisis de riesgos* es una guía enfocada en la evaluación y gestión de riesgos de cumplimiento en pequeñas y medianas empresas (Pymes). Su correcta aplicación puede garantizar la implementación de cualquier norma y mantener los riesgos que la organización enfrenta bajo un control aceptable.

El Protocolo está acompañado de una *Herramienta de autodiagnóstico*, que es un instrumento para evaluar el riesgo de cumplimiento de la normatividad aplicable a empresas de cualquier sector y condición o ubicación geográfica, como Pymes así como cámaras, gremios y asociaciones.² Para el caso que nos ocupa, la herramienta está ejemplificada con riesgos de corrupción contenidos en los artículos 66 a 72 de la Ley General de Responsabilidades Administrativas (LGRA), así como los elementos de control establecidos en el artículo 25 del mismo ordenamiento. Adicionalmente, contempla los seis componentes de evaluación de riesgos contenidos en *A Guide for Anti-Corruption Risk Assessment*,³ de la United Nations Global Compact Office, que son: compromiso del liderazgo; evaluar riesgos, oportunidades e impacto; definir objetivos, estrategias y políticas; implementar estrategias y políticas; medir y monitorear impactos y progresos, y comunicar progresos y estrategias para la mejora continua.

Hay que destacar que aunque el sistema de gestión de riesgos debe ser impulsado por la Dirección General, éste debe ser comprendido, implementado y mantenido en todos los niveles de la organización y por cada individuo que forma parte

¹The United Nations Convention against Corruption, New York, 2013, p. 1

²Ver Anexo Evaluación de Compromiso

³The United Nations Global Compact, 2013, p. 9.

de ella. El reto es hacer de este sistema una herramienta útil y cotidiana, además del fundamento de la cultura empresarial en la toma de decisiones, todo ello con el fin de que su adopción y evolución contribuyan a la maduración de la empresa.

Como ya se mencionó, el presente *Protocolo de análisis de riesgos* y la *Herramienta de autodiagnóstico* representan una propuesta metodológica para la gestión de riesgos de corrupción y se elaboraron junto con una serie de documentos dirigidos a promover la cultura de la integridad en las empresas: un Código de Conducta Modelo y su Manual de Implementación y un Documento de Mapeo y Reporte de Buenas Prácticas. Los acompaña un Glosario para la Integridad Corporativa para facilitar la comprensión de los términos utilizados.

Todos estos productos se desarrollaron en el marco del Proyecto “Apoyando el cumplimiento de los Objetivos de Desarrollo Sostenible en México por medio de prácticas de gobierno abierto, participación ciudadana y el fortalecimiento de la transparencia” implementado por el Programa de las Naciones Unidas para el Desarrollo (PNUD) en conjunto con la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), en apoyo al proyecto “Fortalecimiento y acompañamiento del Programa de Integridad” de la Secretaría de la Función Pública, con el objetivo de proveer herramientas para fortalecer la integridad empresarial y a su vez favorecer el cumplimiento del artículo 25 de la LGRA,⁴ por parte de las pequeñas y medianas empresas (Pymes). En el proceso de elaboración de dichas herramientas, la colabo-

⁴ Artículo 25. En la determinación de la responsabilidad de las personas morales a que se refiere la presente Ley, se valorará si cuentan con una política de integridad. Para los efectos de esta Ley, se considerará una política de integridad aquella que cuenta con, al menos, los siguientes elementos:

- I. Un manual de organización y procedimientos que sea claro y completo, en el que se delimiten las funciones y responsabilidades de cada una de sus áreas, y que especifique claramente las distintas cadenas de mando y de liderazgo en toda la estructura;
- II. Un código de conducta debidamente publicado y socializado entre todos los miembros de la organización, que cuente con sistemas y mecanismos de aplicación real;
- III. Sistemas adecuados y eficaces de control, vigilancia y auditoría, que examinen de manera constante y periódica el cumplimiento de los estándares de integridad en toda la organización;
- IV. Sistemas adecuados de denuncia, tanto al interior de la organización como hacia las autoridades competentes, así como procesos disciplinarios y consecuencias concretas respecto de quienes actúan de forma contraria a las normas internas o a la legislación mexicana;
- V. Sistemas y procesos adecuados de entrenamiento y capacitación respecto de las medidas de integridad que contiene este artículo;
- VI. Políticas de recursos humanos tendientes a evitar la incorporación de personas que puedan generar un riesgo a la integridad de la corporación. Estas políticas en ningún caso autorizarán la discriminación de persona alguna motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas, y
- VII. Mecanismos que aseguren en todo momento la transparencia y publicidad de sus intereses.

ración, liderazgo y compromiso de cada uno de los miembros del Grupo de Trabajo Empresarial (GTE)⁵ ha sido fundamental.

Al igual que el Código de Conducta Modelo y el Manual de Implementación, el Protocolo y la Herramienta de Autodiagnóstico se elaboraron a partir de la información derivada de tres cuestionarios en línea contestados por las empresas afiliadas a las cámaras y asociaciones de categoría que conformaron el GTE de la iniciativa de integridad empresarial.

Los cuestionarios buscaron medir el conocimiento y la aplicación del Programa de Integridad, establecido en el artículo 25 de la LGRA, así como las conductas, aproximaciones y victimización asociadas a la corrupción, con respecto a los siguientes temas: a) Experiencias de riesgos de conductas relacionadas a la corrupción de Pymes; b) Subgrupo para la construcción del Código de Conducta Modelo y su Manual de Implementación; c) Protocolo de Análisis de Riesgos Relacionados a la Corrupción y su Herramienta de Autodiagnóstico.

⁵ Los integrantes del Grupo de Trabajo Empresarial (GTE) están enlistados en el Documento de Mapeo y Reporte de Buenas Prácticas para la Prevención y el Combate a la Corrupción y Promoción de la Integridad en Pymes.

I. Gestión de riesgos

La gestión de riesgos es una meta posible en toda empresa. Se logra mediante la adaptación de una metodología que permite identificar, priorizar, evaluar, medir, monitorear y revisar los riesgos asociados a una actividad, función o proceso, con el fin de administrarlos.

La administración de riesgos se entiende como una evaluación sistemática del riesgo relacionada a cada aspecto relevante de la organización, que proporciona la base para desarrollar e implementar la estrategia de mitigación del riesgo.

Fuente: A Strategy for Safeguarding against Corruption in Major Public Events, The United Nations Convention against Corruption (UNODC).

El control de riesgos es un componente de la identificación y administración de riesgos que involucra la implementación de políticas, estándares y/o procedimientos para eliminar o minimizar los riesgos adversos. Al nivel de empresa, los riesgos pueden ser la consecuencia de factores exógenos (externos a las empresas), endógenos (internos a las empresas) e individuales (que dependen de las acciones y/u omisiones de cada persona).

Fuente: Guía Anticorrupción para las Empresas; Metodologías y definiciones internacionales", Convención de las Naciones Unidas contra la Corrupción (UNODC).

El objetivo final de la Gestión de Riesgos es que la empresa establezca un nivel de tolerancia a cada riesgo.

Bajo este enfoque, una empresa debe determinar cuáles son los riesgos específicos a los que se enfrenta (de cumplimiento, operativos, financieros, etc.) y, a mayor riesgo, asignar más recursos para reforzar los controles.

1.1 ¿Qué es un riesgo?

Un riesgo⁶ es la probabilidad de que ocurra un evento negativo y el efecto o impacto de tal evento, cuya existencia represente una amenaza (fuente de peligro) y vulnerabilidad de la organización a sus efectos. Es decir:
riesgo = probabilidad por impacto.

⁶ Guía de Gestión de Riesgos para las empresas, Cámara Internacional de Comercio (ICC, por sus siglas en inglés).

El análisis de riesgos es el uso sistemático de la información y material disponible para determinar la frecuencia y probabilidad de un posible hecho o circunstancia de riesgo de corrupción, la magnitud de sus posibles consecuencias y la vulneración que se tiene ante ciertas circunstancias. Dicho análisis debe ser constante y continuo, tomando en cuenta el contexto en el cual existe la organización, de evaluación y tratamiento de los riesgos, y de monitoreo de resultados y condiciones de desempeño

Fuente: Glosario de Términos de Integridad Corporativa (Proyecto "Fortalecimiento y acompañamiento del primer componente del Programa de Integridad de la SFP", UNODC, PNUD, SFP), basado en el Estándar Australiano de Administración de Riesgos, apoyado de la ISO 31000-2009 (Herramienta para evaluar la gestión de riesgos).

1.2 Tipos de riesgos

A continuación, se presenta una clasificación de los riesgos que pueden enfrentar las empresas, según la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.⁷

Tipos de riesgos	
Riesgo estratégico	Son los riesgos relacionados con el cumplimiento de los objetivos estratégicos de la empresa y la definición de políticas. (Ejemplo: disminución de ventas o pérdida de clientes.)
Riesgo operativo	Son riesgos asociados a los procesos y a la estructura de la empresa. (Ejemplo: Alta rotación de personal o falta de control de quejas.)
Riesgo financiero	Están vinculados con el manejo de los recursos de la empresa. (Ejemplo: No medir bien la deuda adquirida o la falta de liquidez.)
Riesgo de cumplimiento	Se asocian a la capacidad de la empresa para cumplir requisitos legales y contractuales. (Ejemplo: violar la Ley General de Responsabilidades Administrativas o no cumplir las disposiciones fiscales como el pago de ISR.)
Riesgo de tecnología	Están relacionados con la capacidad tecnológica de la empresa para satisfacer sus necesidades actuales y futuras. (Ejemplo: No contar con un sistema de contabilidad automatizado o falta de capacitación del personal en manejo de sistemas.)

⁷ UNESCO, Bureau of Strategic Planning "Risk Management Training Handbook", 2010.

1.3 Riesgo de cumplimiento

El presente Protocolo es una guía enfocada en la evaluación de riesgos de cumplimiento, que también pueden definirse como los riesgos de sufrir sanciones legales o regulatorias, pérdidas financieras, materiales o reputacionales como consecuencia del incumplimiento de leyes, regulaciones o normas, estándares adoptados por la organización y códigos de conducta, según las actividades de cada empresa.

II. Etapas de la gestión de riesgos de cumplimiento



2.1 Identificar riesgos

La empresa debe realizar un mapeo de las regulaciones nacionales e internacionales que le aplican e identificar las obligaciones y requerimientos que impactan negativamente en sus negocios y en su reputación. Para esta valoración, la empresa puede responder a las preguntas qué, cómo, cuándo y por qué debe cumplir con ellas.

Adaptar una metodología acorde a la empresa. Iniciar e incorporar progresivamente un lenguaje común a la gestión de riesgos en reportes, reuniones, políticas y métricas.

Cruzar Norma *versus* Proceso (Verificar que los procesos cumplan las normas). Comprender procesos y procedimientos para un mejor análisis.

2.2 Priorizar riesgos

En este paso, con base en el conocimiento de la empresa, se evalúa de forma general la normatividad que le aplica, así como las pérdidas financieras por incumplimiento y su impacto en la reputación. Con esta información, se categoriza cada riesgo como Alto, Medio o Bajo (recomendable para Pequeñas y Medianas Empresas). Esto permitirá decidir más adelante los recursos que se asignarán para administrar cada uno.

- ¿Cuáles son los riesgos de los procesos de la empresa?
- ¿En qué actividades específicas de la empresa se encuentran los riesgos?
- ¿Cómo impacta negativamente a las empresas la falta de cumplimiento?

2.3 Evaluar riesgos

En este ejercicio la empresa deberá analizar, en el ámbito de su actividad y de los servicios que presta, dos parámetros: el impacto y la probabilidad de que el riesgo se concrete, lo que se conoce como “riesgo inherente”.

2.3.1 Riesgo inherente

Es el riesgo propio de las actividades y los servicios que presta la empresa, que exceden los controles o mecanismos de prevención existentes. Ejemplos: choques en el transporte, derrumbes en la minería, demandas laborales en una empresa.

- El impacto: se refiere a las consecuencias que deberá enfrentar la empresa en caso de que se materialice el riesgo. En el caso del riesgo de cumplimiento o de corrupción, estas consecuencias pueden ser la pérdida financiera por posibles sanciones impuestas por la autoridad o el daño a la reputación, que se traduce en falta de credibilidad y pérdida de confianza de clientes y/o proveedores.
- La probabilidad: se refiere a la posibilidad de que se produzca el evento de riesgo, sin tomar en consideración los controles o mecanismos de prevención existentes. Para medir esta probabilidad se utilizan criterios de “frecuencia”, es decir, el número de veces que se ha materializado el riesgo en un periodo determinado en el pasado, o criterios de “factibilidad”, es decir, la expectativa de que se materialice en el futuro.

La combinación de ambos parámetros dará como resultado un determinado nivel de riesgo.

Dependiendo del tamaño y la complejidad de la empresa, el rango de los riesgos puede ser SIMPLE o COMPLEJO. Este modelo recomienda para Pymes la calificación ALTO, MEDIO y BAJO

Es indispensable:

- Impulsar desde el más alto nivel la gestión de riesgos.
- Designar a responsables de cada proceso y/o riesgo.
- Capacitar a los responsables en el modelo de gestión de riesgos.

La evaluación de riesgos facilita la toma de decisiones.

2.3.2 Evaluar controles

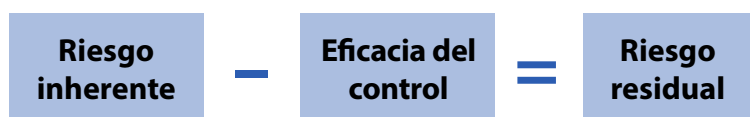
Es el análisis que se realiza para identificar si las medidas de seguridad adoptadas para vigilar los procesos son efectivas y confiables. A partir de esto, se categorizan en ALTO, MEDIO o BAJO.

Todos los controles existentes deben documentarse en políticas y procedimientos. Algunos indicadores (ej. número de quejas, ventas, siniestros) pueden ser utilizados como controles. Identificar el diseño de los controles, si son MANUALES o AUTOMÁTICOS. Un control manual, por lo general, será menos seguro que uno automático, ya que éste elimina el factor de error humano.

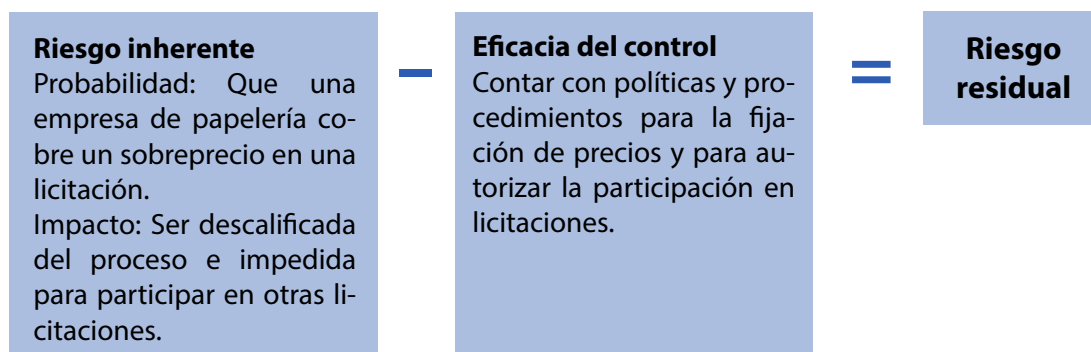
2.3.3 Riesgo residual

Es el riesgo que persiste aún con la aplicación de controles. Es aquél al que realmente se enfrenta la empresa. Podría representarse en la siguiente fórmula:

Riesgo Inherente – Eficacia del Control = Riesgo Residual



Ejemplo:



Una vez completadas todas las fases de la evaluación, la empresa debe decidir qué tipo de respuesta o tratamiento va a dar a cada riesgo: evitarlo, aceptarlo, compartirlo o mitigarlo. Ejemplos de Niveles de Tolerancia:

- Evitar: Dejar de producir o vender un producto.
- Aceptar: Asumir el riesgo con su impacto medido.
- Compartir: Contratar outsourcing o comprar un seguro de daños.
- Mitigar: Establecer límites a las operaciones o fortalecer los procesos.

2.4 Monitoreo

Es necesario monitorear de manera permanente la efectividad de los controles establecidos: si son los adecuados se ratifican, de lo contrario, se modifican.

Se considera que un control es efectivo si arroja alertas sobre fallas en los procesos. Un control no es efectivo, y por lo tanto debe modificarse, si no detecta alertas y por otro medio se identifica una falla en el proceso.

La empresa debe definir la frecuencia del monitoreo (trimestral, semestral, anual, etcétera).

Lo más recomendable es que el monitoreo sea utilizado como una herramienta de autoevaluación, por lo que, en un esquema efectivo, la persona encargada del control debería serlo también del monitoreo y de los cambios que se requieran.

- Todos los riesgos y controles requieren ser monitoreados.
- Los resultados del monitoreo pueden cambiar la priorización y evaluación de un riesgo.
- Los planes de acción deben documentarse.
- La periodicidad del monitoreo depende del riesgo.

Analogía del monitoreo

Al adquirir un auto, y para mantenerlo en condiciones favorables, el usuario deberá monitorear que el riesgo de descompostura no se materialice. Para ello, deberá revisar periódicamente diversos indicadores, entre ellos el nivel de aceite.

Si el medidor está en “verde” (fig. 1), no corre ningún riesgo; si marca “amarillo” (fig. 2), será necesario aplicar un control o medida, como revisar el nivel de aceite.



Figura 1 y 2.

Pero si el indicador se acerca o está en “rojo” (fig. 3), puede ser que el usuario ya no tenga tiempo de llegar al taller o a la gasolinera: se está materializando el riesgo y es alta la probabilidad de que el auto se desviele.



Figura 3.

Conclusión: En la vida diaria se utilizan de manera cotidiana diversas formas de monitoreo, como por ejemplo los análisis de sangre en el cuidado de la salud, o los estados de cuenta de una tarjeta de crédito para controlar el nivel de endeudamiento.

Monitoreo en la empresa

Una empresa que quiera controlar el riesgo de corrupción deberá establecer controles y nombrar a un responsable del proceso, que defina los mecanismos y la frecuencia del monitoreo. Asimismo, deberá generar indicadores confiables que garanticen la efectividad de los controles y, en caso de existir fallas o anomalías, desarrollar planes de acción para mejorarlos.

Por ejemplo, para evitar que el riesgo de corrupción se materialice, se deben monitorear los controles de pagos a terceros mensualmente, y revisar los principales servicios, proveedores, montos y niveles de autorización, emitiendo reportes para su análisis.

2.5 Planes de acción

Esta metodología permite la autocorrección, ya que cuando se identifica que un riesgo no se está mitigando correctamente se elaboran planes de acción, que son aquellas actividades a las que se compromete la administración para subsanar las deficiencias.

Los planes de acción deben cumplir objetivos determinados, ser claros, realistas y contar con fecha de cumplimiento.

2.6 Revisión (testing) y auditoría

La empresa, según sus recursos, puede realizar una revisión o testing de los controles de riesgos, antes de una auditoría.

Revisión (testing)

Se recomienda realizar una revisión o testing, para poner a prueba los controles. Esta revisión debe incluir las pruebas documentales (políticas, procedimientos, manuales, códigos, libros, guías, etc.) y evidencias de registros (contables, de

regalos y entretenimiento, de contratos, declaración de conflicto de interés, etc.) para verificar que se cumpla lo reflejado en la evaluación y el monitoreo.

La revisión también permite verificar si se aplicaron las acciones para corregir las desviaciones detectadas en el monitoreo y la implementación de los planes de acción.

Se propone realizar una lista de reactivos (*checklist*) sobre los controles, que registre las evidencias documentales proporcionadas.

Es aconsejable que esta función NO la realice el responsable del control de riesgos, sino un tercero dentro de la empresa, independiente de dicha labor.

Auditoría

La Auditora Interna es una actividad independiente objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

Tanto las revisiones como las auditorías deben emitir reportes de los riesgos identificados.

El responsable del riesgo deberá tomar acciones de mejora cuando las revisiones o auditorías encuentren deficiencias.

El reporte debe compartirse a todas las áreas que tengan impacto directo en las desviaciones.

En las Pymes, lo recomendable es contratar a un externo para realizar este proceso.

III. Comunicación

Comunicar a la dirección general los reportes sobre el estatus de la empresa es requisito *sine qua non* para garantizar la efectividad y mejora continua del sistema de gestión de riesgos y apoyar la toma de decisiones en las estrategias de negocio.

Los resultados obtenidos en la Herramienta de autodiagnóstico deben incluirse en el reporte ejecutivo.

La dirección general definirá la periodicidad de dichos reportes y su formalidad. Además, deberá asegurarse de que el sistema de riesgos sea una política comprendida, implementada y mantenida en todos los niveles de la organización. (Ver Anexo “Evaluación de compromiso”).

IV. Preguntas y respuestas

1. ¿Es importante que la empresa desarrolle una estrategia de riesgos?
Sí, porque con ella identifica los riesgos residuales a los que está expuesta, lo que le facilita la toma de decisiones y la asignación de recursos.
2. ¿Cuáles son los riesgos de cumplimiento que la empresa debe atender de manera prioritaria? Aquellos que tengan un impacto alto en la organización, una vez analizada la relación entre la normatividad y el cumplimiento de ésta en los procesos de la empresa.
3. ¿Qué debe hacer la empresa con un riesgo inherente Alto?
Implementar controles efectivos que disminuyan dicho riesgo.
4. ¿Qué debe hacer la empresa con un riesgo inherente Medio?
Implementar controles para disminuirlo o aceptarlo con su impacto medido.
5. ¿Qué debe hacer la empresa con un riesgo residual Bajo? Continuar con los controles establecidos que lo mantienen en ese nivel.
6. ¿El riesgo residual debe tomar en cuenta los resultados de auditorías, o cualquier tipo de revisiones, supervisiones o evaluaciones? Sí, porque si el resultado de los reportes fue satisfactorio significa que los controles son adecuados y la probabilidad y el impacto de que se materialice el riesgo están disminuidos. En caso de resultados negativos, es necesario establecer controles o mejorar los existentes.
7. ¿Si la empresa tiene operaciones en otros estados, todas las sucursales deben tener los mismos factores de riesgo y controles?
No necesariamente. Solo si cambia el ramo, las actividades o el entorno en que operan las sucursales (regulación, índice de corrupción y uso de terceros, entre otros.)
8. ¿Qué pasa si los controles manuales que realizo no están reflejados en ningún procedimiento?
Al no existir evidencia documental, se arriesga la continuidad del control. Por ejemplo, si el personal a cargo es reemplazado y el nuevo no tiene manera de conocer el proceso, el riesgo queda expuesto.
9. ¿Los indicadores incorrectos de un área de la empresa pueden impactar en la toma de decisiones de otra?
Sí, desde destinar mayores recursos a un área que no los necesita hasta errores en los estados contables o tomar decisiones equivocadas.
10. ¿Quién debe coordinar los esfuerzos de la gestión de riesgos?

V. Algunos estándares internacionales de gestión de riesgos

El dueño o director general de la empresa es el responsable primero y quien debe delegar esta función.

- ISO 9001 (Gestión de Calidad)
- ISO 3100 (Gestión de Riesgos)
- ISO 19600 (Gestión de Sistemas de Compliance)
- Metodología COSO1 II (Enterprise Risk Management)
- Regulación AS/NZS 4360
- A Guide for Anti-Corruption Risk Assessment (United Nations Global Compact Office)

VI. Comentarios de metodología

El presente Protocolo de Riesgos y la Herramienta de Autodiagnóstico asociada fueron diseñados para auxiliar a las Pymes a observar la legislación en materia de anticorrupción en la gestión de riesgos de cumplimiento.

De acuerdo con la Ley General de Responsabilidades Administrativas, los particulares pueden incurrir en faltas administrativas graves como soborno, participación ilícita en procedimientos administrativos, tráfico de influencias, utilización de información falsa, colusión, uso indebido de recursos públicos y contratación indebida de recursos públicos (Arts. 66 al 72). Todas estas faltas administrativas se incluyen en la Herramienta de Autodiagnóstico como sus riesgos de Corrupción.

Los controles establecidos en la herramienta referida, son los mismos que establece el artículo 25 de la LGRA: Manuales de organización y procedimientos, Código de conducta, Sistemas adecuados y eficaces de control, vigilancia y auditoría, Sistemas adecuados de denuncia, Sistemas y procesos de entrenamiento y capacitación, Políticas de recursos humanos y Mecanismos que aseguren en todo momento la transparencia y publicidad de sus intereses.

Las medianas y grandes empresas que cuenten ya con un sistema de gestión de riesgos de cumplimiento implementado pueden utilizar el Protocolo y la Herramienta en la capacitación e introducción del sistema de riesgos a sus colaboradores.

Hay que destacar que esta metodología puede utilizarse para otros riesgos de cumplimiento, como privacidad y antilavado de dinero.

VII. Anexo

Check list de evaluación de compromiso

Este listado es una propuesta de formato para que las cámaras, gremios y asociaciones obtengan de sus afiliados el compromiso de implementar un sistema de gestión de riesgos

Compromiso	Cumplido Sí / No / En proceso
La empresa identifica los riesgos de conductas relacionados a la corrupción.	
La empresa define prioridades a partir de la identificación del riesgo.	
La empresa evalúa los riesgos y documenta los resultados.	
La empresa monitorea los resultados de la evaluación de riesgos.	
La empresa prueba los controles para garantizar su eficacia.	
La empresa desarrolla un plan de acción e implementa controles para minimizar riesgos.	

Empresa: _____

Nombre del responsable: _____

Firma: _____

Fecha: _____

