INFORME
Nº 4

Guía para la elaboración de matrices de riesgo

Programas de Integridad Ley 27.401

COMISIÓN DE INTEGRIDAD Y CUMPLIMIENTO

Consejo Profesional
de Ciencias Económicas
de la Ciudad Autónoma
de Buenos Aires

consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires

GUÍA PARA LA ELABORACIÓN DE MATRICES DE RIESGO

Informe N° 4

Incluye modelo de Matriz de Riesgo en soporte digital

Comisión de Integridad y Cumplimiento

Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires

Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires
Guía para la elaboración de matrices de riesgo ; Coordinación general de Gabriela Verónica Russo. - 1a ed. - Ciudad Autónoma de Buenos Aires : Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires, 2023.
Libro digital, PDF - (Informes de comisión ; 4)

Archivo Digital: descarga
ISBN 978-987-660-390-4

1. Análisis de Riesgo. 2. Prevención de Riesgos. I. Russo, Gabriela Verónica, coord.
CDD 330.82

Hecho el depósito que marca la Ley 11.723.

Consejo Profesional de Ciencias Económicas de la
Ciudad Autónoma de Buenos Aires
Viamonte 1549 - CABA
Tel. 5382-9200
www.consejo.org.ar

ÍNDICE

La elaboración de la presente Guía ha estado a cargo de la Comisión de Integridad y Cumplimiento del Consejo Profesional de Ciencias Económicas de la CABA.

Presidente: Dr. Raúl Saccani

Vicepresidente: Dr. Mariano Fernandez

Consejero Coordinador: Dr. Oscar Fernandez

Han participado de la producción los miembros de la Comisión:
Dr. Claudio Borsetti y Dra. Paula D'Onofrio.

Se incluye un Ejemplo Básico de una matriz de riesgo en Excel elaborada por el Dr. C.P. Claudio Borsetti, a la que puede acceder haciendo clic aquí.
La sigla "**EB**" (Ejemplo Básico) se utiliza a lo largo del texto para indicar cuándo puede consultar la Matriz de riesgo en Excel para facilitar y mejorar la comprensión de su estructura y sus mapas de colores.
Este libro de Excel tiene el poder de acelerar significativamente sus esfuerzos de aprendizaje e implementación de la matriz de riesgo y será una herramienta indispensable de estudio y referencia a medida que avance en el proceso de construcción de la matriz.

1. INTRODUCCIÓN

El profesional en Ciencias Económicas tiene formación académica en áreas que guardan relación cercana con la labor que se espera de alguien que evalúe un Programa de Integridad (por ejemplo, el análisis de riesgos y los controles internos, entre otros). En esta línea, una de las condiciones relevantes para el ejercicio profesional radica en la independencia con respecto a la información/área/ente motivo del encargo.

La Comisión de Integridad y Cumplimiento, en el marco de la línea prevista por el Consejo Profesional de Ciencias Económicas, ha venido trabajando activamente en los temas relacionados con el desarrollo de conceptos técnicos, con la capacitación y con la sensibilización acerca de la importancia que tiene para la profesión abordar las labores relacionadas con este ámbito de actuación.

Se suma a dicho trabajo esta publicación, que viene a plantear una cuestión central como son las Matrices de Riesgo.

Muchos de los colegas matriculados han recibido consultas de sus clientes en relación con los programas de integridad previstos en lo establecido en la Ley 27.401 - Responsabilidad Penal de las Personas Jurídicas. Uno de los elementos fundamentales para el armado y posterior demostración de su razonable funcionamiento consiste en confeccionar una matriz de riesgo proactiva y de acuerdo con el contexto de la organización.

Cabe mencionar también el desarrollo de la figura de *Compliance Officer* u Oficial de Cumplimiento como rol o área de consulta respecto de las medidas y herramientas de ética, transparencia y cumplimiento normativo en una organización. Este rol, que se ubica en la segunda línea de defensa, debe contar con formación especializada, como la que adquieren los profesionales en Ciencias Económicas en las carreras de grado y posgrado. Tanto desde una perspectiva de diseño, monitoreo o evaluación, la prevención de la corrupción en la órbita de las personas jurídicas es una materia donde diferentes profesiones pueden hacer su aporte, dado que la actuación interdisciplinaria de profesionales de las ciencias jurídicas y sociales, las buenas prácticas de negocios, la indagación e investigación, las técnicas de comunicación, la gestión de riesgos y la gestión de personas resultan cruciales para un buen Programa de Integridad, que sea sólido, efectivo y adecuado.

El presente Programa de Trabajo tiene por objetivo asistir al profesional matriculado para que esté en condiciones de diseñar una matriz de riesgos, realice su evaluación e identifique los riesgos de corrupción como parte fundamental del Programa de Integridad. También, por ejemplo, para ejecutar la debida diligencia de terceras partes. Esta práctica que realizan las compañías para, entre otros, verificar la identidad de sus clientes, proveedores, etc. cumpliendo con las exigencias legales y las normativas y reglamentaciones vigentes. Puede tener como objetivo la solicitud de un peritaje, o bien, una evaluación independiente solicitada por el mismo cliente.

La matriz es propia de cada organización y se elabora en función de la actividad, su dimensión y los factores internos y externos que la afectan. Cada organización deberá elaborarla conforme a los requisitos en materia de cumplimiento que puedan estar originados en la existencia de partes interesadas internas o externas (vale decir, personas u organizaciones que pueden afectar, verse afectadas, o percibirse como afectadas por una decisión o actividad del ente en cuestión).

El alcance de la matriz deberá proyectarse en cuanto a geografía, sujetos, actividades y cobertura de sus principales riesgos (es decir: su perímetro técnico y su exposición a los riesgos). Es importante

que en su diseño se involucren los diversos actores: el compromiso de la alta dirección para transmitir la importancia de un proceso de evaluación y la capacitación del personal para que puedan identificar su posible exposición a prácticas corruptas.

Dr. Oscar Fernandez
Tesorero del CPCECABA
Consejero Coordinador de la Comisión de Integridad y Compliance

2. LA GESTIÓN DE RIESGOS EMPRESARIALES
Antecedentes

La gestión de riesgos empresariales tal y como la conocemos hoy no es un concepto nuevo en la literatura económico-empresarial, ya que su origen se circunscribe -décadas atrás- al ámbito de los seguros.

Si bien es cierto que las primeras compañías aseguradoras datan de finales del siglo XVII y principios del XVIII, fue tras la Segunda Guerra Mundial cuando las organizaciones comenzaron a suscribir masivamente pólizas para protegerse frente a riesgos cuya materialización podía afectar de manera negativa a la operativa de la empresa y, por ende, al logro de sus objetivos. Los riesgos a los que se daba cobertura eran, generalmente, aquellos derivados de accidentes, incendios, inundaciones, naufragio de naves o catástrofes naturales.

Así las cosas, en los años 50 era habitual que muchas compañías reclutasen a profesionales que tenían como misión exclusiva la contratación y gestión de pólizas de seguros. Eran los denominados "*insurance buyers*" o "*insurance managers*". De este modo, la gestión de riesgos consistía, básicamente, en la transferencia de la responsabilidad de una empresa a la compañía aseguradora, que sería quien, en última instancia, respondiese económicamente de los daños o pérdidas derivados de la materialización de un determinado riesgo.

En este escenario, muchos profesionales tomaron conciencia de que estas medidas "correctivas" suponían un gasto ingente para las organizaciones que destinaban una buena parte de sus presupuestos a esta partida. Así fue como empezó a emerger la idea de que, si los riesgos empresariales se gestionasen de una manera más proactiva en el seno de la compañía, no sería necesario depender exclusivamente de las entidades aseguradoras. Así pues, el *insurance buyer* se convirtió progresivamente en el *risk manager*, un profesional que gestionaba los riesgos a través de la identificación y la evaluación previa, buscando fórmulas para su tratamiento dentro de la propia organización.

Con el paso de los años, la función de gestión de riesgos ha ido evolucionando hasta que en los años 90 comenzaron a surgir modelos de gestión y control de riesgos empresariales que tienen por finalidad servir de pauta a las organizaciones a la hora de identificar, evaluar y gestionar sus riesgos de manera efectiva.

Actualmente, los mercados de capitales están volcando su enfoque de riesgos hacia la evaluación de temáticas ambientales, sociales y de gobernanza, también conocido como riesgos **ASG** o **ESG** (según sus siglas en castellano o en inglés). Dentro de estos últimos se encuentran los relacionados con la mencionada ley y serán objeto de nuestro análisis.

3. CONSIDERACIONES GENERALES

3.1 Concepto de riesgo

Con carácter general, puede definirse el riesgo como:
(i) Contingencia o proximidad de un daño;
(ii) posibilidad de que una persona o cosa sufra un daño o perjuicio;
(iii) posibilidad de que ocurra una desgracia o un contratiempo, o
(iv) exponerse al fracaso o a un peligro.

Según estas definiciones, el riesgo implica una probabilidad o posibilidad de que se produzca un determinado daño, por lo que, cuando hablamos de riesgo, existe una falta de certeza sobre unos eventos que no sabemos si se van a producir o no. O, en otras palabras, cuando hablamos de riesgos, hablamos de la probabilidad de que se materialice el daño en la exposición.

En todo caso, aunque parezcan conceptos similares y en ocasiones se utilizan indistintamente, debemos distinguir el riesgo del peligro, ya que, a los efectos que nos ocupan, son cuestiones distintas. Así pues, el peligro es aquella situación que *per se* ya representa una amenaza, mientras que el riesgo es la exposición a esa amenaza. Por este motivo, los peligros se identifican, mientras que los riesgos se evalúan.

Gráficamente es sencillo apreciar esta diferencia:

Si trasladamos estas consideraciones al ámbito empresarial, nos encontramos con muchas definiciones de riesgos empresariales que toman la falta de certeza, la incertidumbre o la probabilidad como elemento clave del concepto.

Así, por ejemplo, el *Committee of Sponsoring Organizations* (COSO) define el riesgo empresarial como:

"La posibilidad de que ocurran eventos que afecten a la consecución de la estrategia y objetivos empresariales".

Por su parte, la norma internacional ISO 31000:2018 (Gestión del riesgo. Directrices) define el riesgo como "el efecto de la incertidumbre en los objetivos".

Entremos en detalle en los tres elementos de la definición de riesgo en la norma: efecto, incertidumbre y objetivos:

Se precisa que un **efecto** es "una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades o amenazas".

El término **incertidumbre** "es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad".

Tal y como se muestra en la figura siguiente, el grado de conocimiento de las probabilidades y de las consecuencias se podrá definir en cuatro zonas de incertidumbre, quedando el riesgo restringido a la zona donde las consecuencias están bien definidas y se tiene alguna base para estimar las probabilidades.

Relación entre los conceptos de riesgo e incertidumbre

Los **objetivos** "pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles". Ejemplos de estos aspectos (financieros, de salud y seguridad o ambientales) y de los niveles (estratégico, de proyecto, de producto, de proceso o de organización completa).

Los objetivos de la organización pueden tener diferentes alcances:

- Organización: incluye administraciones públicas, entes privados, comunidades emprendedoras, asociaciones, grupos o individuos.
- Los objetivos de sus partes interesadas.
- Los objetivos de la sociedad en su conjunto.

La verdadera gestión del riesgo es mucho más que números; es el arte de utilizar las herramientas cuantitativas para gestionarlo realmente. El riesgo es un componente central, tal vez "el más central", de la gestión de una organización. Pero administrar el riesgo, dice Coleman, tiene algo de doble personalidad (Coleman, 2012). El riesgo es tanto el arte de gestionar personas, procesos e instituciones como la ciencia de medir y cuantificar el riesgo.

Las bases subyacentes para pensar, debatir y medir el riesgo pueden y deben ser coherentes en las distintas divisiones y niveles de una organización. Aunque la información debe adaptarse adecuadamen-

te, es importante que los fundamentos -la forma en que se concibe y calcula el riesgo- sean coherentes desde el nivel granular hasta el nivel agregado. La medición del riesgo, su lenguaje, incluso la propia definición, todo ello puede variar drásticamente entre los niveles de una empresa[1].

Gestionar el riesgo exige pensar en él, y hacerlo nos obliga a reflexionar sobre la incertidumbre y la aleatoriedad, y a sentirnos cómodos con ellas. Resulta que, como seres humanos, a menudo somos malos para pensar de forma probabilística. Preferimos la certidumbre en nuestras vidas y pensar en el azar no es algo natural; la probabilidad no suele ser intuitiva[2]. Ahora bien, a nadie le sorprende especialmente que se requiera un análisis cuantitativo para informar, guiar y corregir la intuición. El pensamiento estadístico (y probabilístico) sólido puede mejorarse, a través de la formación y con herramientas y técnicas adecuadas, mediante tres pasos (Gigerenzer, 2002):

1. Derrotar la ilusión de certeza (la tendencia humana a creer en la certeza de los resultados o en la ausencia de incertidumbre).
2. Conocer los riesgos reales de los acontecimientos y acciones relevantes.
3. Comunicar los riesgos de forma comprensible.

Estos también se aplican a la gestión de riesgos de Compliance. La mayor parte del trabajo en gestión de riesgos se centra en el segundo -aprender sobre los riesgos-, pero el primero y el tercero son igualmente relevantes. Pensar en la incertidumbre es difícil, pero es importante reconocer que ocurren cosas inesperadas; el futuro es incierto. Y comunicar el riesgo es especialmente importante.

3.2 Tipos de riesgos en las organizaciones

Las organizaciones se enfrentan, en su día a día, a numerosos riesgos de muy diversa índole y con diferente alcance. Así pues, existen, por un lado, una serie de riesgos que pueden tener un impacto negativo en la empresa si bien no le impiden en modo alguno la consecución de sus objetivos (ej.: una caída temporal de la red de datos). Se trata de riesgos que a corto plazo pueden tener alguna consecuencia negativa o poco deseable para la sociedad (pérdida de ventas, insatisfacción del consumidor), pero que en modo alguno amenazan la continuidad del negocio.

Por otro lado, existen otro tipo de riesgos cuyo impacto negativo es mucho más significativo, ya que conllevan considerables pérdidas y afectan directamente a la consecución de objetivos y que, en ocasiones, abocan a la propia empresa a su desaparición (ej.: caso ENRON).

Así las cosas, existen numerosas clasificaciones sobre los diferentes tipos de riesgos empresariales que atienden a muy diversos criterios. Nosotros hemos decidido catalogarlos -únicamente- en los siguientes grupos:

- Estratégicos
- Financieros
- Legales/regulatorios
- Operacionales
- Reputacionales

En todo caso, un mismo riesgo puede incardinarse en varias de estas categorías a la vez, e incluso la gran mayoría, por no decir todos ellos, pueden conllevar implícitamente un riesgo reputacional, ya que

[1] La coherencia ofrece dos ventajas. En primer lugar, la alta dirección puede tener la seguridad de que, cuando gestiona el riesgo de toda la empresa, en realidad está gestionando la agregación de los riesgos de las unidades individuales. En caso necesario, los altos directivos pueden desglosar las fuentes de riesgo. En segundo lugar, los responsables de cada unidad pueden saber que, cuando un alto directivo les plantea una pregunta sobre su riesgo, esta se refiere al riesgo que están gestionando realmente (Coleman, 2012).

[2] El azar impregna nuestro mundo. La experiencia y la formación no siempre nos preparan para comprender o convivir cómodamente con la incertidumbre. De hecho, toda una industria y una literatura se basan en estudiar cómo la gente comete errores al pensar y juzgar la probabilidad (Coleman, 2012).

cualquier riesgo mal gestionado puede traer consecuencias negativas para el buen nombre o la reputación de la empresa.

3.2.1 Riesgos estratégicos

No hay una definición "estándar" o ampliamente aceptada acerca de qué es riesgo estratégico. Nosotros definiremos el riesgo estratégico como:

"el impacto negativo que puede tener en una organización una incorrecta decisión empresarial, un plan de negocios fallido o la falta de capacidad de respuesta a los cambios en sector, industria o territorio en el que se opera".

Ejemplo: una compañía que quiere introducir un determinado producto en el mercado y se dirige a un segmento incorrecto de población. Una estrategia enfocada erróneamente puede derivar en sustanciales pérdidas (riesgo estratégico y operacional).

Ahora bien, como señalamos anteriormente, un riesgo estratégico puede ser al mismo tiempo un tipo de riesgo que puede englobarse en cualquiera de las otras categorías. Los riesgos estratégicos pueden proceder de variables internas o externas a la organización. Entre las primeras se encuentra la propia estrategia, entendida como el conjunto de planes, medidas y medios elegidos por una organización para alcanzar sus metas y objetivos. Mientras que las variables externas son las amenazas consustanciales al contexto en el que opera la organización y que, en ocasiones, son muy difíciles de prever y evaluar, lo que complica anticiparse a su materialización, y ello hace que, en ocasiones, no esté preparada para afrontarlos y gestionarlos. En la medida en que estos riesgos están directamente ligados a la estrategia empresarial, sus propietarios suelen ser los órganos de gobierno de las organizaciones, generalmente, alta dirección y órgano de administración.

A pesar de la importancia de este tipo de riesgos y que, en ocasiones, puede poner en peligro la propia supervivencia de la empresa, la atención que las organizaciones prestan a este tipo de riesgos es muy escasa si se compara con el tiempo dedicado al análisis de riesgos operacionales, financieros o legales.

Adicionalmente, las pérdidas causadas por los riesgos estratégicos superan considerablemente las originadas por otras categorías de riesgo, ya que las primeras representan casi un 90% del total de las causadas por otros riesgos.

3.2.2 Riesgos operacionales

El riesgo operacional hace alusión, generalmente, a una falla inesperada en las operaciones diarias de una empresa. Falla que puede deberse a un factor humano, procesos internos inadecuados o fallidos, o incluso a eventos externos que escapan del ámbito de control de la empresa. Algunos de los riesgos operacionales más comunes son, entre otros:

i) riesgos relacionados con la ciberseguridad (ciberataques, hackeo, robo de datos);

ii) fallas en los procesos internos de la empresa (fallas de maquinaria, inadecuados procesos de control);
iii) riesgos relacionados con los empleados, proveedores y clientes (poca formación, error humano, falta de diligencia debida en la selección de proveedores);
iv) riesgos asociados al entorno socioeconómico y geopolítico (cambio en la situación política de un país o en la regulación que nos impide operar en las circunstancias actuales, condiciones ambientales catastróficas).

A modo de ejemplo, a continuación, se enumera el listado de los riesgos operativos que más han preocupado al sector financiero y bancario en el año 2020:

- Ciberseguridad
- Protección de datos
- Robo y fraude
- Subcontratación y riesgo de tercera parte
- Resiliencia
- Cambio organizacional
- Comportamientos poco éticos o irregulares
- Riesgo regulatorio
- Gestión del talento
- Riesgo geopolítico

3.2.3 Riesgos financieros

Los riesgos financieros son, probablemente, los que gozan de una mayor cobertura en la literatura sobre gestión de riesgos empresariales. Este tipo de riesgo se ha definido de muy diversas maneras, entre otras:

i) la probabilidad de ocurrencia de un evento que tenga consecuencias financieras negativas para una organización;
ii) la capacidad de una compañía para gestionar su deuda;
iii) la capacidad de una compañía para hacer frente a sus obligaciones.

Algunos factores que pueden afectar al riesgo financiero de una compañía son, entre otros, los siguientes:

i) fluctuación en el precio de las acciones;
ii) devaluación;
iii) tipos de interés;
iv) inflación.

Sea como fuere, el riesgo financiero hace referencia a la capacidad de una compañía de generar el flujo de caja suficiente para hacer frente al pago de intereses sobre su financiación o para cumplir otras obligaciones relacionadas con su deuda. Una compañía con un nivel de deuda relativamente alto conlleva un mayor riesgo financiero en la medida en que aumentan las posibilidades de que la compañía no sea capaz de afrontar sus obligaciones financieras y pueda devenir insolvente.

Existen muchos tipos de riesgos financieros y diversas clasificaciones de estos.

Los principales riesgos financieros pueden resumirse en los siguientes:

- Riesgo de crédito: se denomina también riesgo de contraparte ya que hace referencia a la incertidumbre, asociada a la falta de cumplimiento por parte del deudor de los pagos a su vencimiento. Así pues, ante el impago de un crédito puede haber un impacto negativo en la organización debido a la disminución del flujo de caja o a los gastos derivados del proceso de la reclamación del pago o del proceso de recobro.
- Riesgo de liquidez: aquel que se refiere a la incapacidad de una empresa de tener suficiente efectivo o activos convertibles rápidamente en efectivo para hacer frente a sus obligaciones.

Este riesgo tiene una doble cara o vertiente. Por un lado, el riesgo de liquidez de activos, esto es, que, a pesar de disponer de un activo y queriendo disponer de él, no es posible materializar su compra o se hace a un precio muy inferior al que normalmente se haría. Y, por el otro lado, está el riesgo de liquidez de pasivos cuando estos no se satisfacen a la fecha de vencimiento o, de hacerse, se hacen a un precio inadecuado.

- Riesgo de cambio: es la exposición a la que se enfrentan las organizaciones que operan en diferentes países en relación con las pérdidas o ganancias impredecibles con motivo del cambio en el valor de una moneda en relación con otra divisa.
- Riesgo de mercado: hace referencia a la probabilidad de que se produzca una pérdida de valor de una cartera, o portafolio financiero, producida por los cambios en las variables de mercado (tasas de interés, tasas de cambio de moneda, *spreads* de crédito).

3.2.4 Riesgos legales

El riesgo legal o de cumplimiento puede definirse como el riesgo a recibir sanciones legales o reglamentarias, pérdida financiera o daño a la reputación, resultante del incumplimiento de las leyes, reglamentos, normas, otros requisitos reglamentarios o códigos de conducta, y otras normas de las organizaciones autorreguladas.

Dentro del riesgo de cumplimiento o riesgo legal existen diversas modalidades. Por ejemplo, el riesgo contractual es el riesgo que tiene la organización de sufrir pérdidas o consecuencias negativas con motivo del incumplimiento de un contrato por la contraparte. El riesgo no contractual, por su parte, es el impacto negativo en una organización derivado de los daños causados a un competidor, un cliente o un tercero con el motivo de la infracción de las normas que regulan el ejercicio de su actividad (ej.: infracción de los derechos de propiedad industrial o intelectual).

También en el marco de los riesgos legales se habla de riesgo de litigio para referirse al riesgo que tiene una organización de ser demandada ante los tribunales ordinarios de justicia. La lista de razones por las que puede ser una empresa demandada es interminable y van desde motivos relacionados con empleados (discriminación, acoso, despidos) hasta temas fiscales (impago de impuestos) o medioambientales (delito contra la naturaleza), entre otros.

Por último, mencionaremos lo riesgos regulatorios que afectan en mayor medida a aquellas empresas de sectores o industrias sometidos una "hiperregulación" legislativa con motivo de su actividad (medicamentos, cosméticos, alimentos, etc.). Este riesgo es aquel derivado de la incertidumbre que producen los cambios y novedades legislativas en las diversas jurisdicciones en las que opera una empresa.

3.2.5 Riesgo reputacional

Como su propio nombre lo indica, el riesgo reputacional es el potencial daño que se puede ocasionar al buen nombre o la buena reputación de una empresa, que puede surgir de malas prácticas o de comportamientos ilícitos o irregulares por su parte o por parte de sus empleados. Podríamos decir que se trata del único riesgo que es común a todas las empresas, ya que es el activo intangible más valioso de cualquier organización.

4. LA CORRUPCIÓN Y LA LEY 27.401

4.1 ¿Qué se entiende por corrupción?

Definición de *Transparency International*:
"Abuso del poder encomendado para beneficio privado".

Definición de la Real Academia Española:
"Es la práctica consistente en la utilización de las funciones y medios de las organizaciones, especialmente las públicas, en provecho, económico o de otra índole, de sus gestores".

Definición del Programa Global de Naciones Unidas en contra de la corrupción:
"Abuso de poder para fines privados".

Definición de la Convención de Corrupción Civil del Consejo Europeo:
"Solicitar, ofrecer, otorgar o aceptar, directa o indirectamente, un soborno o cualquier otra ventaja indebida del mismo, lo que distorsiona el desempeño adecuado de cualquier deber o comportamiento requerido del receptor del soborno o la ventaja indebida del mismo".

Definición del Banco Mundial:
"Ofrecer, dar, recibir o solicitar, directa o indirectamente, cualquier cosa de valor para influir indebidamente en las acciones de la otra parte".

4.2 ¿Qué se entiende por soborno?

El delito de soborno o cohecho es uno de los delitos más comunes de corrupción. Prueba de esto es la ISO 37001, publicada en 2016, como el primer estándar internacional para sistemas de gestión antisoborno. La norma se ha dirigido a facilitar a las organizaciones implementar y mantener medidas concretas que les permitan prevenir, detectar y abordar el soborno y las prácticas fraudulentas en sus actividades comerciales. También podemos mencionar la Ley antisoborno del Reino Unido, que a menudo se describe como la legislación en materia anticorrupción más dura del mundo, aunque solo se centra en el delito de soborno.

La doctrina suele diferenciar las figuras delictivas de cohecho en pasivo y activo según el punto de vista que se aborda: pasivo del funcionario que acepta o solicita una promesa o dádiva para realizar un acto relativo a su cargo, y activo del particular que corrompe al funcionario con sus ofrecimientos y dádivas.

Definición de *Transparency International*:
"La oferta, promesa, entrega, aceptación o solicitud de una ventaja, es un incentivo para una acción ilegal, no ética o una violación de la confianza. El incentivo puede tomar la forma de obsequios, préstamos, tarifas, recompensas u otras ventajas (impuestos, servicios, donaciones, favores, etc.)".

Definición de ISO 37001:16:

"La oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (financiero o no financiero), directa o indirectamente, independientemente de la ubicación, en violación de la ley aplicable como un incentivo o recompensa para una persona que actúa o se abstiene de actuar en relación con el desempeño de los deberes de esta".

4.3 La evaluación del riesgo y la Ley 27.401

Si bien la evaluación del riesgo constituye una herramienta necesaria en cualquier organización, es claro que, con la promulgación de la Ley 27.401 de Responsabilidad Penal de las Personas Jurídicas, se ha incrementado su puesta en funcionamiento si realmente queremos prevenir la corrupción dentro de nuestra organización.

Los delitos tipificados por la mencionada ley son: cohecho, soborno transnacional, tráfico de influencias, negociaciones incompatibles con el ejercicio de la función pública, concusión, enriquecimiento ilícito y balances e informes agravados. Por su parte, el riesgo evaluado por la norma es la posibilidad de que se realice un acto de corrupción en nombre, beneficio o interés de la empresa, sin importar si el mismo es realizado por alguien interno o externo a la organización.

La Ley determina que el programa deberá contener, "al menos", los siguientes elementos:

- Un código de ética o de conducta, o la existencia de políticas y procedimientos de integridad aplicables a todos los directores, administradores y empleados, independientemente del cargo o función ejercidos, que guíen la planificación y ejecución de sus tareas para prevenir la comisión de los delitos bajo la Ley 27.401.
- Reglas y procedimientos específicos para prevenir ilícitos en el ámbito de concursos y procesos licitatorios, en la ejecución de contratos administrativos o en cualquier otra interacción con el sector público.
- Capacitaciones periódicas sobre el programa de Compliance a directores, administradores y empleados.

Adicionalmente, la ley establece que el programa "podrá" contener los siguientes elementos:

- Análisis periódico de riesgos y la consecuente adaptación del programa de integridad.
- Apoyo visible e inequívoco al programa de integridad por parte de la alta dirección y la gerencia.
- Canales internos de denuncia de irregularidades, abiertos a terceros y adecuadamente difundidos.
- Una política de protección de denunciantes contra represalias.
- Un sistema de investigación interna que respete los derechos de los investigados e imponga sanciones efectivas a las violaciones del código de ética o conducta.
- Procedimientos que comprueben la integridad y trayectoria de terceros o socios de negocios, incluyendo proveedores, distribuidores, prestadores de servicios, agentes e intermediarios, al momento de contratar sus servicios durante la relación comercial.
- La debida diligencia durante los procesos de transformación societaria y adquisiciones, para la verificación de irregularidades, de hechos ilícitos o de la existencia de vulnerabilidades en las personas jurídicas involucradas.
- El monitoreo y evaluación continua de la efectividad del programa de integridad.
- Un responsable interno a cargo del desarrollo, coordinación y supervisión del programa de integridad.
- El cumplimiento de las exigencias reglamentarias que sobre estos programas dicten las respectivas autoridades del poder de policía nacional, provincial, municipal o comunal que rija la actividad de la persona jurídica.

Sugerimos para ampliar el contenido general de los programas de integridad remitirse a: Informe 1: Aspectos prácticos y preguntas frecuentes en la implementación de Programas de Integridad.

Informe 2: Guía para la implementación de programas de Integridad https://www.consejo.org.ar/storage/attachments/InfoN%C2%BA2-Comisi%C3%B3nAnticorrupci%C3%B3n.pdf-uX4JNYvhVq.pdf

Informe 3: Beneficio Indebido: Un análisis preliminar https://archivo.consejo.org.ar/publicacionesedicon/Informe3-Beneficio-Indebido-Un-Analisis-Preliminar-Anticorrupcion.pdf publicados por la Comisión de Integridad y Cumplimiento del CPCECABA.

Como vemos, la evaluación de riesgos no se encuentra mencionada como mandatoria. Sin embargo, el análisis de riesgo continuo no es un elemento más. Si la evaluación inicial de riesgos es presupuesto esencial de la adecuación del Programa, el análisis periódico de riesgos es un elemento vital para corroborar si lo que una vez resultó adecuado continúa siéndolo en el presente.

Cuando la empresa/entidad ya posee una política, procedimientos y responsables de una gestión de riesgos en general, es deseable que el análisis periódico de los relacionados con el cumplimiento de la Ley se integre a ellos. Si aún no lo tiene, es imprescindible que comience con este proceso.

Si bien dicha ley es de un significativo progreso para abordar el soborno y la corrupción, ella por sí sola no es suficiente para resolver el problema, que requiere un alto nivel de responsabilidad de las organizaciones para contribuir de manera proactiva para combatir la corrupción, en particular en su *supply chain* integral y la tercerización o subcontratación de sus procesos para prevenir y mitigar el riesgo de corrupción.

El abordaje y la priorización de los riesgos de corrupción deberían subyacer en el diseño del Programa de Integridad y permitir en el futuro explicar su cómo y el por qué. Una correcta evaluación de riesgos ayuda a determinar si una medida de prevención resulta efectiva para la organización.

Poder evaluar el impacto de todo comportamiento que pueda involucrar a la organización en una investigación, atraer el interés de autoridades de control o causar un impacto negativo en la reputación de la organización (aún si no se tiene la certeza de que sea realmente un delito), es relevante al momento de considerar los riesgos de corrupción y sus consecuencias.

5. RIESGOS ESG - RIESGOS DE GOBERNANZA/ COMPLIANCE

Los riesgos relacionados con factores ESG o ASG son los riesgos y/u oportunidades relacionadas con factores medioambientales, sociales y de gobierno que pueden causar un impacto en una entidad. No existe una definición universal de los riesgos relacionados con factores ESG, a los que también se los puede denominar riesgos de sostenibilidad, riesgos no financieros o extrafinancieros, pero que también de manera indirecta podrían impactar financieramente. Cada entidad tendrá sus propias definiciones basadas en su modelo empresarial específico; el entorno interno y externo; la combinación de productos o servicios; la misión, visión y valores clave, y demás.

Cuando hablamos de riesgos medioambientales, podemos pensar en consecuencias del cambio climático, impacto sobre los recursos naturales, la polución y residuos (en cualquiera de sus formas), y oportunidades medioambientales que podríamos recibir del Estado o de entidades que apoyan nuestras medidas amigables con el ambiente.

Los mencionados como riesgos sociales se refieren a temas tales como capital humano, responsabilidad sobre el producto, oposición de las partes interesadas y oportunidades sociales. También incumben a temas de Derechos Humanos, normativas laborales en la cadena de suministro, cualquier exposición al trabajo infantil ilegal y otras cuestiones más rutinarias, como el cumplimiento de la política de salud y seguridad en el trabajo. La calificación social sube también si una empresa está bien integrada en su comunidad local y por ello cuenta con una «licencia social» para operar con consentimiento; esto se produce en relación con las interacciones con los diferentes grupos de interés.

Los denominados riesgos de "gobernanza" se refieren a las buenas prácticas en el gobierno y la conducta corporativa. Es decir: una serie de reglas o principios que definen los riesgos, responsabilidades y expectativas entre las diferentes partes interesadas en cuanto al gobierno de las organizaciones. Un sistema de gobierno corporativo bien definido se puede utilizar para equilibrar o alinear los intereses entre las partes interesadas y puede funcionar como una herramienta para respaldar la estrategia a largo plazo de una empresa. Temas relativos a las remuneraciones de la alta gerencia, auditorías, evaluaciones de control y riesgos, *reporting*, conflicto de intereses y políticas de transparencia y prácticas para evitar la corrupción son algunos de los temas que podría abarcar.

Existen numerosos ejemplos de factores ambientales, sociales y de gobierno corporativo (ASG), y estos están en constante evolución. Los siguientes son algunos de ellos:

Ambientales	Sociales	De gobierno corporativo
▪ Cambio climático	▪ Derechos Humanos	▪ Soborno y corrupción
▪ Agotamiento de recursos	▪ Formas modernas de esclavitud	▪ Compensación del equipo ejecutivo
▪ Residuos	▪ Trabajo infantil	▪ Diversidad y estructura de las juntas directivas
▪ Contaminación	▪ Condiciones laborales	▪ Cabildeo o «lobby» político y donaciones
▪ Deforestación	▪ Relaciones con los empleados	▪ Estrategia fiscal

Fuente: principios para la inversión responsable PNUMA-PACTO GLOBAL.

Como ejemplos concretos podemos ver los presentados por la guía COSO-WBCSD, que han tenido impacto a nivel internacional, pero que podrían aplicarse a cualquier actividad en particular.

Fuente: guía COSO –WBCSD.

En los mercados de capitales estos riesgos son tenidos en cuenta y los inversores cada vez piden más información relacionada con la sostenibilidad. En particular existe una creciente atención de los grandes inversores institucionales hacia la inversión responsable y a saber cómo las empresas están abordando los desafíos en materia social y medioambiental para lograr un crecimiento sostenido a largo plazo. Claramente, el interés por las empresas, más allá de la rentabilidad de estas, se relaciona con la sostenibilidad en el tiempo.

Sin embargo, es interesante lo que plantea un informe de las empresas alineadas al WBCSD (Consejo Mundial de empresarios para el Desarrollo Sostenibilidad), donde se señala una serie de factores que impiden una buena rendición de estos:

- La dificultad a la hora de cuantificar los riesgos relacionados con factores ESG en términos monetarios. No hacerlo complica en gran medida la priorización y la asignación apropiada de recursos, particularmente cuando el riesgo se presenta a largo plazo con impactos indeterminados que emergen a lo largo de un período de tiempo desconocido.
- La falta de conocimiento de los riesgos relacionados con factores ESG en una entidad y la limitada colaboración interdisciplinaria entre los profesionales de la gestión del riesgo y de la sostenibilidad.
- Los riesgos relacionados con factores ESG son gestionados y divulgados por un equipo de especialistas en sostenibilidad y se consideran como riesgos separados o menos importantes que los riesgos estratégicos, operativos o financieros convencionales, lo que da lugar a una serie de sesgos contra los riesgos relacionados con factores ESG (*Sustainability* and ERM: *The first step towards integration*).

Según el marco de ERM de COSO, el valor de una entidad se crea, preserva, erosiona o materializa sobre la base de la relación entre los beneficios derivados de los recursos desplegados y el coste de estos recursos. El valor de una entidad está determinado en gran medida por las decisiones que toma la dirección: desde las decisiones de la estrategia general hasta las más cotidianas. Históricamente, este valor se ha medido principalmente a través de los factores financieros y económicos que afectan a los bienes

tangibles de la entidad. No obstante, esto ha cambiado muy rápido. El concepto de valor se ha ampliado también hasta englobar los recursos compartidos entre una entidad y la sociedad en general. El capital ya no es un término del que se habla en singular, pues ha evolucionado hasta hablarse de múltiples valores y flujos de capitales, reconociendo la variedad de recursos de los que dependen las organizaciones.

Los cinco componentes del marco de ERM de COSO comienzan con «gobierno y cultura» y «estrategia y establecimiento de objetivos», pasando luego a los procesos de ERM que se centran en el «desempeño» (identificar, evaluar y priorizar, y dar respuesta a los riesgos) y culminan con la «revisión y monitorización», y la «información, comunicación y *reporting* de los riesgos».

En este informe haremos referencia a metodologías, como las del informe COSO ERM, donde la implementación de dichos procesos permite identificar, evaluar, gestionar, monitorizar y comunicar los riesgos, incluso los relacionados con factores ESG.

Los riesgos relacionados con factores ESG son tan relevantes para las pequeñas y medianas empresas como para las grandes corporaciones o los organismos gubernamentales. No obstante, dado que las PyME tienen recursos limitados, es lógico que adapten los mismos de manera eficiente.

Afianzando esta línea, el capítulo argentino del Pacto Global y la Cámara Argentino-Alemana ha desarrollado una Guía de Integridad Sostenible https://pactoglobal.org.ar/novedades/integridad-sostenible-el-primer-programa-acelerador-orientado-al-ods-16-en-argentina/, que permite abordar de manera integrada las distintas problemáticas: respetar los derechos humanos, asegurar los estándares laborales, cuidar el ambiente y luchar contra la corrupción. Para esto, dentro del Programa de Integridad Sostenible se propone el desarrollo conjunto de una matriz de riesgo que evalúe los riesgos:

"Partiendo de este nuevo concepto, se propone la formación de un equipo interdisciplinario que sume a la mesa de trabajo, además de las áreas de Legales, Control Interno, Gestión de Riesgos y Cumplimiento Normativo, a los responsables de Integridad, de Sostenibilidad, de Recursos Humanos, Operaciones y Compras. Con la finalidad de lograr el establecimiento de políticas y procedimientos internos de manera armoniosa, obteniendo la sinergia no solo para cumplir con la legislación vigente y disminuir la responsabilidad de las empresas sino también con la visión y compromiso de generar verdaderos efectos en las sociedades y el planeta". Guía de Integridad Sostenible https://pactoglobal.org.ar/novedades/integridad-sostenible-el-primer-programa-acelerador-orientado-al-ods-16-en-argentina/

La Agenda Global 2030, con sus 17 objetivos, nos sirve como guía y brújula para vincular los impactos en las diferentes áreas de las tres dimensiones (Ambiental, Económica y Social).

Específicamente, en lo que al ODS 16 se refiere, podemos mencionar la meta 5 "Reducir considerablemente la corrupción y el soborno en todas sus formas"; la meta 6 "Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas".

Si pretendemos un desarrollo que satisfaga las necesidades de la generación presente, sin comprometer la capacidad de las generaciones futuras de satisfacer sus propias necesidades, dediquemos un espacio a reflexionar:

¿Qué rol desempeñan la ética y la integridad en la gestión de los recursos públicos?

¿Cuán permeable es nuestra cultura organizacional a la hora de diseñar un código de conducta sistémico alineado a los ODS para el Desarrollo Sostenible?

¿Prestamos atención a las tendencias a la hora de desarrollar un Programa de Integridad que satisfaga los atributos necesarios?

¿Conocemos el mapa de nuestras partes interesadas o grupos de interés? ¿Quiénes son? ¿Qué rol e incidencia juegan actualmente?

Es de suma conveniencia considerar diferentes variables relevantes a la hora de implementar y gestionar las actividades de las organizaciones, con un abordaje proactivo y estratégico desde Compliance, y en conjunto con otras áreas de la organización.

Las buenas prácticas en las organizaciones contribuyen más allá del ODS 16 de la Agenda 2030.

Erradicar la corrupción es vital para lograr el desarrollo sostenible. Y desde la profesión de Ciencias Económicas contamos con diferentes herramientas para contribuir a este objetivo internacional, de alto impacto en la economía y bienestar de las personas y organizaciones.

Por eso, si bien es importante tener un enfoque amplio de los riesgos, en esta primera etapa centraremos nuestro trabajo en los riesgos relacionados con la corrupción, específicamente, de acuerdo con los mencionados en la Ley 27.401.

El perfil de riesgo de corrupción en una empresa se crea a partir del contexto donde desarrolla sus actividades, en el cual se consideran factores, como la ubicación, el sector, el ámbito regulatorio, los socios de negocio/terceras partes, las operaciones con gobiernos extranjeros, las relaciones con funcionarios o terceros en países en los que no existen regulaciones estrictas sobre las prácticas corruptas.

Algunos indicadores que deben monitorearse, ya que pueden ayudar a detectar dónde podrían ser propensos a cometer actos de corrupción son:

- Falta de conocimientos de riesgos aparejados o hechos de corrupción por deficiencias de formación, capacitación y habilidades de los empleados.
- Fallas en los sistemas de premios propensos a comisión de delitos de corrupción.
- Falta de políticas y procedimientos claros, especialmente en lo relativo a gastos de representación, gastos de promoción, obsequios, contribuciones políticas.
- Falta de controles financieros y no financieros eficaces.
- Falta de liderazgo ético de la alta dirección y, en consecuencia, de un mensaje conciso y decidido sobre el soborno y la corrupción desde arriba.
- Conductas influenciables o proclives para cometer ilícitos en un marco de políticas poco claras sobre conductas éticas.
- Escaso o nulo ambiente de control.
- Falta de sistemas de castigos o sanciones concretas.
- Falta de transparencia y seguridad de los canales de denuncias.
- Falta de políticas claras de protección a los denunciantes.
- Escasa o nula respuesta a las denuncias, o bien demoras en la implementación del análisis de los casos que termina desestimulando el uso del canal de denuncias.
- Falta de control en los negocios con el Estado y funcionarios públicos.
- Falta de control en los negocios a través de socios de negocio/terceras partes (facilitadores), con familiares (conflictos de intereses-nepotismo).

6. GESTIÓN DEL RIESGO: normas y estándares internacionales

Si bien no es posible eliminar todos los riesgos, es responsabilidad de la organización demostrar que los riesgos empresariales se han identificado adecuadamente y que también se han tomado las medidas oportunas para prevenirlos. Por lo tanto, la gestión de riesgos se puede definir como el proceso de identificar, evaluar y controlar las amenazas/riesgos de una organización.

La gestión integral de riesgos empresariales ha ido ganando una gran importancia en las últimas décadas. Así pues, desde que se aprobase el marco COSO, han ido surgiendo numerosas normas, guías y estándares internacionales que sirven de guía para el diseño y la elaboración de los modelos de gestión y control de riesgos en las organizaciones. Aunque sería imposible mencionar todos ellos, a continuación, destacamos aquellos más comunes.

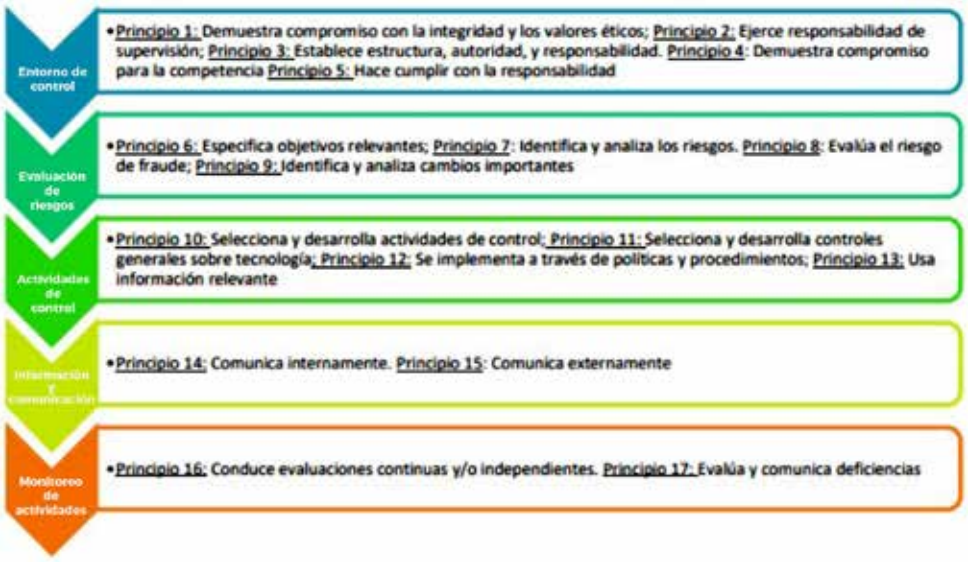
6.1 Marco COSO. Gestión integrada del riesgo

El modelo COSO-ERM (*Enterprise Risk Management-Integrated Framework*) es uno de los más utilizados en la gestión de riesgos empresariales y sirve de marco de referencia en relación con tres aspectos fundamentales en el seno de las organizaciones:

(i) la gestión de riesgos;
(ii) el control interno;
(iii) la prevención del fraude.

El modelo de control interno COSO 2013 (COSO III) está compuesto por los cinco componentes (que ya figuraban en el marco anterior) y 17 principios que recogen las características fundamentales de cada componente. Los cinco componentes del modelo de control interno son los siguientes:

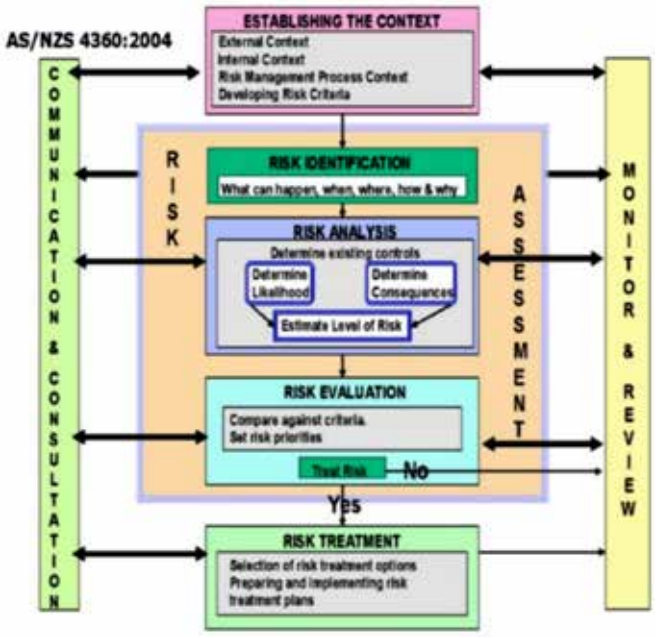
Junto con estos cinco componentes, el marco integrado recoge 17 principios que muestran las características fundamentales de cada uno de los componentes del control interno y que deben de tenerse en cuenta para el diseño e implantación de un sistema de control interno eficaz:



6.2 El estándar AS/NZS 4360:2004

El estándar australiano/neozelandés (AS/NZS 4360:2004) diseña un proceso de gestión de riesgos a través de una serie de fases o subprocesos, a saber:

i) establecimiento del contexto;
ii) identificación de riesgos;
iii) análisis de riesgos;
iv) evaluación de riesgos;
v) tratamiento de los riesgos.

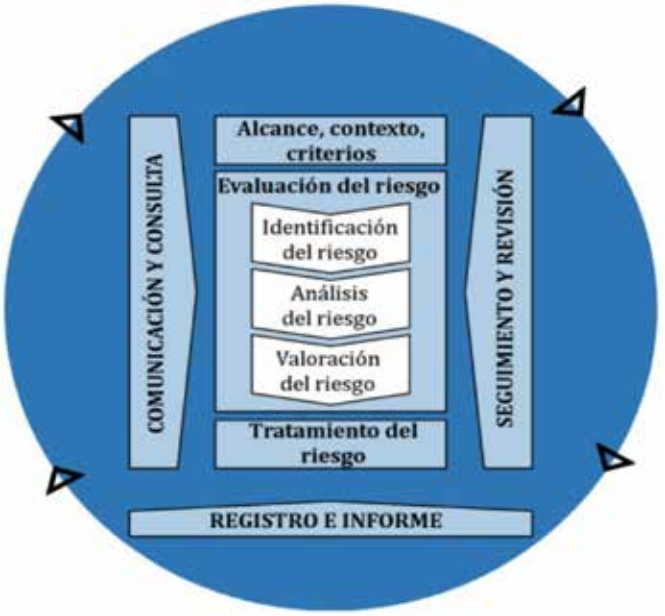


6.3 La ISO 31000. Gestión del riesgo

El estándar internacional ISO 31000:2018, bajo la rúbrica "Gestión de riesgos. Principios y Directrices", establece los parámetros o pautas para la gestión del riesgo en el seno de las organizaciones públicas y privadas con independencia de su tamaño y el sector en el que operan, ya que no se trata de una norma específicamente dirigida a una industria en concreto. Así pues, debido a su carácter global y comprehensivo, utilizaremos esta norma como referencia para la identificación, análisis y evaluación del riesgo a la hora de diseñar un sistema de gestión de Compliance.

Según este estándar internacional, el proceso de gestión del riesgo consiste en la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consultoría, estableciendo el contexto y la evaluación, tratamiento, seguimiento, revisión, registro y comunicación de riesgos.

Gráficamente, el proceso de gestión del riesgo sería el siguiente:



Así pues, el propósito de la gestión del riesgo es la creación y protección de valor. Mejora el rendimiento, estimula la innovación y apoya el logro de los objetivos.

Estructura de la norma

ISO 31000:2018

Estructurada en 6 apartados (en lugar de los 9 de la versión anterior):

- 1. Objeto y campo de aplicación.
- 2. Referencias normativa.
- 3. Términos y definiciones.
- 4. Principios.
- 5. Marco de trabajo.
  - 5.1 Generalidades.
  - 5.2 Liderazgo y compromiso.
  - 5.3 Integración.
  - 5.4 Diseño.
  - 5.5 Implementación.
  - 5.6 Evaluación.
  - 5.7 Mejora.
- 6. Proceso.
  - 6.1 Generalidades.
  - 6.2 Comunicación y consulta.
  - 6.3 Alcance, contexto y criterios.
  - 6.4 Apreciación del riesgo.
  - 6.5 Tratamiento del riesgo.
  - 6.6 Seguimiento y revisión.
  - 6.7 Registro y presentación de informes.

7. LA EVALUACIÓN EFICAZ DEL RIESGO

La evaluación de riesgos de corrupción, definida en términos generales, abarca la variedad de mecanismos que utilizan las empresas para estimar la probabilidad de formas particulares de corrupción dentro de la empresa y en las interacciones externas, y el impacto que dicha corrupción podría tener.

Una evaluación de riesgos eficaz significa comprender la empresa, hacer preguntas de manera amplia, comprender los entornos en los que opera y comprender con quién está tratando, tanto en el sector público como en el privado. También significa comprender cómo funcionan en la empresa varios programas y controles anticorrupción y su efecto sobre los riesgos. Solo entonces la empresa puede dirigir los recursos de cumplimiento a su mejor uso.

La evaluación eficaz del riesgo lucha contra la corrupción y no debe ser un evento aislado y único. El despliegue continuo de recursos de la manera más eficaz requiere una comprensión actual y precisa de los riesgos. Para muchas organizaciones esto significará evaluaciones de riesgo anuales; otras pueden completar las revisiones con menos frecuencia, dependiendo de sus perfiles de riesgo y recursos. También puede haber eventos desencadenantes, como la entrada a nuevos mercados, reorganizaciones importantes, fusiones y adquisiciones que crearán oportunidades e incentivos para actualizar y evaluar el riesgo.

Si bien puede que no sea necesario realizar una evaluación integral de riesgos con más frecuencia que una vez al año o incluso cada dos años, es imperativo monitorear continuamente los aspectos más riesgosos de la empresa y permanecer atentos a los eventos, relaciones e interacciones que puedan ocurrir y que pueden aumentar o crear nuevos riesgos.

Es el negocio de toda empresa comprender y responder a los innumerables riesgos que enfrenta, incluyendo no solo la variedad de riesgos de cumplimiento y regulatorios, sino también los desafíos operativos, competitivos y financieros que la gerencia enfrenta todos los días.

Se describe a continuación cada una de las etapas de la evaluación de riesgos:

7.1 Establecer el proceso

Se describen los diferentes elementos de una evaluación de riesgo de corrupción junto con un enfoque para realizar la evaluación. El objetivo de esta sección es proporcionar un enfoque estructurado para realizar una evaluación de riesgos de corrupción en una empresa siguiendo los pasos descritos anteriormente.

Dado que cada empresa tiene una exposición diferente a los riesgos de corrupción, los pasos describen un enfoque genérico, utilizando eventos y riesgos de corrupción comunes como ilustraciones, y sugieren diferentes formas de identificar y evaluar los riesgos.

7.1.1 Comprensión del problema

Una sólida comprensión de los riesgos de corrupción, las causas que pueden afectar el cumplimiento de los objetivos y las posibles consecuencias de incumplimientos derivados de actividades de corrupción son un requisito previo para una evaluación de riesgos sensata.

Se podría considerar un taller inicial, preparado por el departamento legal, de gestión de riesgos, de cumplimiento o de auditoría interna, ya sea facilitado por especialistas externos en corrupción, o no, para explorar los riesgos de corrupción con más detalle.

El objetivo de la reunión es abordar el tema de la corrupción, reconocer que la organización podría estar expuesta a riesgos de corrupción e identificar las factores internos y externos para explorar la exposición al riesgo de corrupción.

7.1.2 Planificación

Una lluvia de ideas de una o dos horas es una buena práctica para una evaluación del riesgo de corrupción, pero una evaluación sólida generalmente implica múltiples actividades para identificar su exposición al riesgo, incluidas preguntas como:

- ¿Quién es el dueño del proceso y debe participar?
- ¿Cuánto tiempo se invertirá en el proceso (planificación, incluyendo hitos, entregables, fechas de decisión)?
- ¿Cómo se recopilarán los datos?
- ¿Qué recursos internos y externos se necesitan?
- ¿Qué análisis adicional se debe realizar?
- ¿Qué metodología se va a utilizar?

7.1.3 Objetivos, partes interesadas y recursos

Se podría realizar una evaluación del riesgo de corrupción por varias razones. Estas deben considerarse en la etapa de planificación para ayudar a diseñar una evaluación que pueda lograr los objetivos subyacentes. En general, el objetivo principal es comprender mejor la exposición al riesgo de corrupción de la empresa para que se pueda tomar decisiones sobre la gestión del riesgo. Otros objetivos pueden incluir:

- Establecer la agenda o las prioridades de las actividades anticorrupción.
- Definir un plan de acción o indicadores clave de desempeño (KPI) para iniciativas anticorrupción.
- Medir el progreso o la eficacia de iniciativas anticorrupción anteriores.
- Sensibilizar sobre los riesgos de corrupción a las partes interesadas claves involucradas en el proceso.
- Monitorear el desarrollo de riesgos de corrupción, analizar tendencias.

7.1.4 Definición de los criterios y tolerancia al riesgo

El concepto de los criterios de riesgo son los "términos de referencia respecto a los que se evalúa la importancia de un riesgo".

Esta definición va acompañada de dos notas importantes:

- Nota 1: Los criterios de riesgo se basan en los objetivos de la organización y en el contexto externo e interno.
- Nota 2: Los criterios de riesgo se pueden obtener de normas, leyes, políticas y otros requisitos.

En definitiva, los criterios de riesgo son los que nos deben servir como referencia para asignar un nivel de riesgo y, en última instancia, tomar decisiones respecto a como actuar con él (tratamiento del riesgo).

Por otro lado, cabe destacar que el concepto de criterio de riesgo engloba los tradicionales conceptos de apetito, capacidad y tolerancia al riesgo.

Una forma muy resumida de interpretar estos conceptos sería:

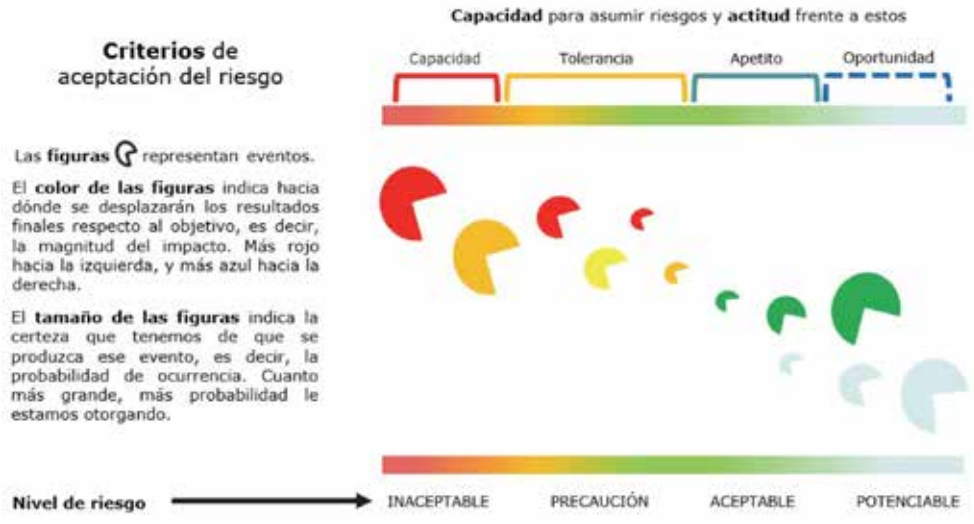
- El apetito por el riesgo será la cantidad de variabilidad que se está dispuesto a asumir sin tomar ninguna medida concreta al respecto.
- La tolerancia al riesgo será la cantidad de variabilidad que, pudiéndose asumir, podría comprometer la consecución del objetivo si no se actuase.

- La capacidad de riesgo sería la cantidad de variabilidad a partir de la cual, en caso de no actuar, se pone en compromiso cierto la consecución del objetivo.

Así, fijado un objetivo como un rango de resultados posibles con el que sentirse satisfecho, el tradicional apetito vendría determinado por la cantidad de variabilidad identificada que sería asumible, sin hacer nada para minimizarla, para acabar dentro de un rango de valores dado, aunque fuera en la parte más baja o más alta.

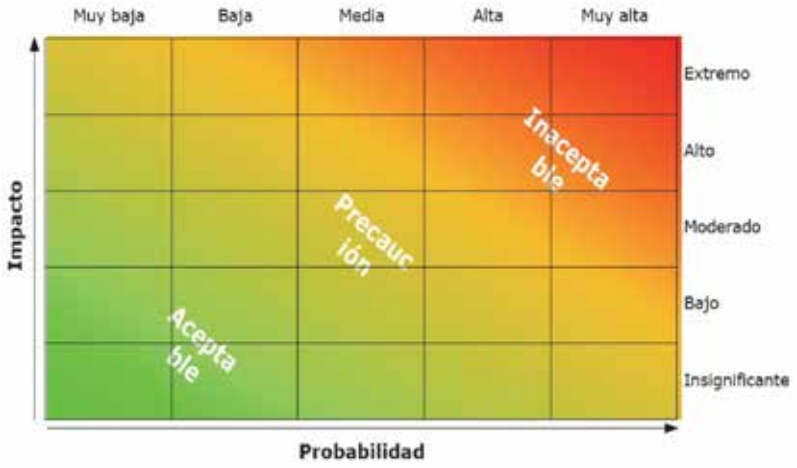
Finalmente, el nivel de riesgo es un elemento cuya determinación deberemos tener en cuenta para fijar los criterios.

Dado que todos estos conceptos (apetito, tolerancia, capacidad, criterio y nivel) vistos de forma conjunta suelen generar confusión, intentaremos aclararlos con la siguiente figura:



La idea consiste en poner una etiqueta a cada riesgo identificado y caracterizado, lo que con posterioridad nos permitirá decidir qué hacer con él. Estas etiquetas serán las que se van a considerar como nivel de riesgo, y son términos descriptivos: inaceptable, inasumible, aceptable, a considerar, precaución.

Así, para convertir unos criterios en un nivel, es necesario generar algún tipo de regla relacional. Es decir, se utilizan unos criterios para asignar un valor a un riesgo para luego decidir si ese valor tiene uno u otro nivel de riesgo. Este aspecto se ve en las tradicionales matrices de riesgo que se muestran en la siguiente figura:



Si nos fijamos, lo que viene a representar esta matriz es que los criterios del riesgo que se utilizan son la probabilidad de ocurrencia y la severidad de las consecuencias. Es decir, lo que posiciona un riesgo en particular dentro del cuadro son su probabilidad y su impacto.

Ahora bien, ¿qué es lo que hace que un riesgo identificado acabe cayendo en el nivel de aceptable o de inaceptable? Precisamente, los criterios del riesgo. Es decir, los criterios del riesgo son las reglas que se utilizarán para asignar valores a los riesgos y así poder definir qué nivel le corresponde a cada uno.

En consecuencia, las organizaciones deberán definir la magnitud y el tipo de riesgo que puede o no ser tomado.

Es valioso determinar el nivel de tolerancia al riesgo en una etapa temprana del proceso de evaluación de riesgos de corrupción, involucrando a la alta dirección.

Si la tolerancia o el apetito por el riesgo no estuvieran definidos, al menos se esperaría que la organización tuviera definidas y comunicadas formalmente escalas de probabilidad y consecuencia, las cuales deberían ser consideradas para el análisis de los riesgos y la elaboración de matrices de riesgo que permitan a la organización establecer prioridades de tratamiento de los riesgos.

Varios incidentes importantes de corrupción en el pasado han involucrado situaciones en las que, en retrospectiva, la gerencia asumía más riesgos de corrupción de los que la alta dirección sabía y hubiera considerado tolerables. Establecer la tolerancia al riesgo por adelantado puede ayudar a que la evaluación de los riesgos residuales sea un ejercicio relativamente sencillo y objetivo. Si la tolerancia al riesgo no se determina explícitamente desde el principio, existe la posibilidad de que la gerencia racionalice los niveles existentes de riesgos de corrupción como aceptables, lo que socavará el propósito y el valor de la evaluación de riesgos de corrupción.

Los participantes pueden plantear preguntas difíciles relacionadas con la tolerancia al riesgo, por ejemplo:

- ¿Cómo es posible que la gerencia diga que tiene cierta tolerancia o apetito por el riesgo de corrupción cuando la alta dirección también afirma tener tolerancia cero con la corrupción?

Una respuesta simple a esto es que la prevención de la corrupción es un arte imperfecto, por lo que cierto nivel de riesgo de corrupción es inevitable a pesar de que la alta dirección puede estar completamente comprometida con evitar la corrupción y defender su afirmación de tener tolerancia cero con los actos de corrupción.

Al evaluar los riesgos de corrupción, la gerencia considera si el nivel de riesgo para cada evento de riesgo de corrupción está dentro de la tolerancia o el apetito de riesgo de corrupción de la alta dirección.

Además de las organizaciones más grandes, el concepto de tolerancia al riesgo es muy importante para las empresas pequeñas o medianas, ya que estas suelen tener recursos limitados y no pueden invertir en todas las mejores prácticas y controles anticorrupción.

El establecimiento de una tolerancia al riesgo permitirá a estas organizaciones a tener un medio para identificar qué riesgos son más críticos e importantes para que se concentren y asignen los recursos escasos.

7.1.5 Registros de riesgo

Durante la etapa de planificación de la evaluación de riesgos de corrupción, es importante determinar cómo se documentará la evaluación de riesgos. Un enfoque común y práctico es identificar y documentar cada categorización, su evento y las causas del riesgo e incluirlo en un "Registro de riesgos".

Este Registro de riesgos también se utilizaría para documentar: el evento de cada riesgo, sus causas y consecuencias, y las calificaciones, así como los programas y controles que mitigan cada uno.

Durante la etapa de identificación del riesgo de una evaluación del riesgo de corrupción, hay beneficios de identificar información detallada para cada evento, como las partes potenciales que pueden perpetrar ese evento (tanto desde dentro de la organización como por los socios de negocio). Además, si hay más de un programa/control que mitiga el evento de riesgo, el registro capturaría los diferentes programas y controles que mitigan ese evento.

De acuerdo con la visión de la *UK Office of Government Commerce* se definen diferentes categorizaciones de riesgo, evento y causas que puedan afectar el cumplimiento de los objetivos de las organizaciones relacionadas con la corrupción:

Categorización de los riesgos de corrupción	Eventos de riesgos de corrupción
Riesgos estratégicos - factor interno: son los que amenazan generar una "interrupción brusca" en la estrategia anticorrupción de la organización. Un riesgo estratégico puede tomar la forma de un evento potencial que pueda menoscabar la implementación de una estrategia o el logro de las metas estratégicas anticorrupción.	• No proporcionar un alto nivel de integridad, calidad y fiabilidad del servicio. • No asegurar políticas y prácticas antisoborno y anticorrupción, mientras se realizan operaciones, proyectos o actividades comerciales. • No asegurar la incorporación del respeto al Código de Ética y Política de tolerancia cero frente a la corrupción, así como el cumplimiento de los requisitos legales nacionales contra el soborno y otros requisitos en la concienciación del personal y la cultura de la organización en general. • No asegurar que la política que prohíbe el soborno y la corrupción esté formalmente documentada y disponible públicamente para todos los empleados, socios de negocios y partes interesadas. • Incumplimiento de que los socios de negocios respeten la política antisoborno y anticorrupción de la entidad y los requisitos del programa de integridad, así como el cumplimiento de las leyes y regulaciones nacionales contra la corrupción. • No asegurar la percepción pública y la reputación de la entidad en lo que respecta a cultura de Compliance en sus objetivos y obligaciones de Compliance. • No asegurar que el liderazgo demuestre un respaldo firme y explícito al programa antisoborno y anticorrupción, y exprese una tolerancia 0 en una declaración pública formal. • Incumplimiento del liderazgo en definir el alcance, la extensión y el compromiso activo del programa. • Falta de gestión de las prioridades del proceso de lucha contra el soborno y la corrupción debido a la falta de una gestión adecuada del personal clave y los socios de negocio. • Fallar en no aprovechar las oportunidades para desarrollar nuevas soluciones proactivas contra el soborno y contribuir a mejorar la integridad y las prácticas, y la cultura anticorrupción en todo el país.

Categorización de los riesgos de corrupción	Eventos de riesgos de corrupción
Riesgos operacionales - Riesgos de incumplimiento de Compliance - Factores internos: surgen dentro de la organización, son controlables y deben eliminarse o evitarse. Algunos ejemplos son los riesgos de las acciones no autorizadas, ilegales, poco éticas, incorrectas o inapropiadas de los empleados y gerentes, y los riesgos de fallas en los procesos operativos de rutina (riesgo de los recursos humanos de la entidad, relacionado con la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo y apropiación de información sensible, entre otros).	• No impedir el soborno a un funcionario público. • No impedir que prácticas corruptas asignen a socios de negocio favoreciéndolos sobre base del nepotismo u otras prácticas ilegales en violación de la evaluación de riesgos de la entidad y el proceso de debida diligencia. • Fallar en determinar y asegurar las competencias (educación, formación y experiencia) de las personas que realizan un trabajo que afecta el desempeño de Compliance. • Fallar en emitir y publicar una política clara, visible y accesible de las obligaciones de Compliance. • Fallar en capacitar o dar asesoramiento a personal y a terceras partes sobre cómo lidiar con el incumplimiento de Compliance • Comprometer o malversar los fondos de la entidad a través de firmas de contratos ineficientes o con eventos de riesgo de sobornos. • Fallar en controlar que los informes financieros sean deliberadamente manipulados. • Fallar en controlar que se produzca malversación de activos tangibles o intangibles (por ejemplo, reembolsos indebidos). • No asegurar la detección de conflicto de intereses que afecta a varias etapas del proceso definido en el alcance. • Violar los requisitos de la responsabilidad individual por la exactitud e integridad de los informes financieros. • Fallar en controlar prácticas de lavado de dinero, etc.

Categorización de los riesgos de corrupción	Eventos de riesgos de corrupción
Riesgos relacionados con socios de negocio/terceras partes - Factores Externos/Internos: sujetos cuya conducta puede afectar negativamente a la organización en términos de reputación.	• Fallar en asegurar la participación de los socios de negocio/terceras partes a la política de tolerancia cero al soborno y la corrupción de la entidad. • Incumplimiento de los socios de negocio/terceras partes para garantizar la prestación de servicios contratados en lo que respecta a la integridad, Compliance, calidad y confiabilidad del servicio o producto • Incumplimiento por parte de socios de negocio/terceras partes de los requisitos legales y reglamentarios locales de anticorrupción y Compliance. • Incumplimiento de los requisitos para la evaluación de riesgos efectiva. • Compromiso y traición deliberados, filtración intencional de información de la entidad o datos confidenciales realizados por proveedores o personal tercerizado. • No garantizar que se comprometa la política de Compliance, el acuerdo de confidencialidad y la declaración de conflicto de intereses de las terceras partes a través del contrato de prestación de servicios y productos. • No asegurar una evaluación de desempeño continuo y adecuado de las terceras partes de la entidad a través del proceso de prestación de servicios y la capacitación y la evaluación de competencias, etc.
Riesgos financieros/Desarrollo económico a nivel nacional - Factores Externos: son los asociados a agentes humanos o físicos no relacionados con la entidad y a su control sobre ella (terceros). Las organizaciones no pueden evitar que ocurran tales eventos. Su gestión debe centrarse en la identificación (tienden a ser obvios en retrospectiva) y la mitigación de su impacto.	• Cambios en las políticas gubernamentales nacionales: esto puede afectar negativamente en los proyectos de funcionamiento del Programa de Integridad • La competencia puede generar impactos en la reputación de la organización por comunicación negativa en redes sociales, etc. • Riesgo de corrupción o incumplimientos por el hecho de no pagar impuestos y dejar de cumplir o sobornar para no pagar más. • Denuncias, litigios judiciales y/o administrativos por incumplimiento: la entidad podría ser objeto de litigios en caso de que se notifique de denuncias de hechos de corrupción en nombre de la organización y que deba defenderse (demostrar su Programa de Integridad) para demostrar que el perpetrador actuó en beneficio propio. • Problemas macroeconómicos que potencien la comisión de delitos de corrupción (dentro de una de las categorizaciones de fraude) al encontrar el perpetrador un ámbito propenso al aumentar la racionalización y la motivación.

Categorización de los riesgos de corrupción	Eventos de riesgos de corrupción
Riesgos legales/ contractuales/regulatorios (legislativo) - Factores externos: son los asociados a agentes humanos o físicos no relacionados con la entidad y con su control sobre ella (terceros).	• Negativa o extorsión al otorgar un permiso o una licencia. • Introducción inesperada de requisitos reglamentarios o de licencia. • Enmiendas en la legislación fiscal. • Introducción inesperada de requisitos reglamentarios o de licencia. Modificaciones en la legislación fiscal.
Riesgos Organizacionales/ Gestiones/Relacionado con los recursos humanos - Factores internos: surgen dentro de la organización, son controlables y deben eliminarse o evitarse. Algunos ejemplos son los riesgos de las acciones no autorizadas, poco éticas, incorrectas o inapropiadas de los empleados y gerentes, y los riesgos de fallas en los procesos operativos de rutina.	• Prácticas inadecuadas en la política corporativa y prácticas de la entidad. • Personal corrompible. • Personal no seleccionado correctamente. • Sistema de premiación que promueve prácticas ilegales. • Sistema de castigo que no se cumple. • Empleados en áreas de alto riesgo de corrupción o de ser sobornados. • Empleados acostumbrados a métodos de venta relacionados con el lobbismo. • Bajo nivel de motivación del personal para la ejecución de los proyectos. • Ineficiente formación y toma de conciencia sobre la gestión de riesgos y los requisitos anticorrupción. • Subestimación de los factores políticos y de mercado (por ejemplo, gestión de riesgos y lucha contra la corrupción).
Riesgos políticos/sociales globales - Factores externos: son los asociados a agentes humanos o físicos no relacionados con la entidad y con su control sobre ella (terceros).	• Saltar procesos de selección definidos por políticas o que se adjudicaron a la opción no más conveniente (proveedor del Estado en productos de primera necesidad en escenarios especiales como la pandemia (ej.: lo que sucedió con las vacunas, barbijos, ambulancias, y muchos insumos ante la urgencia). • Información incorrecta en los medios de comunicación que afecta la imagen de la organización, hechos de corrupción, acoso, etc.
Riesgos ambientales - Factores externos: son los asociados a agentes humanos o físicos no relacionados con la entidad y con su control sobre ella (terceros).	• Catástrofes ambientales provocadas por el hombre por mala gestión ambiental y daños a la propiedad que deriven en sanciones (inundaciones, tormentas, contaminación radiactiva, derrame de petróleo, etc.).

Categorización de los riesgos de corrupción	Eventos de riesgos de corrupción
Riesgos de fallas tecnológicas - Factores internos: surgen dentro de la organización; son controlables y deben eliminarse o evitarse. Algunos ejemplos son los riesgos de las acciones no autorizadas, incorrectas o inapropiadas de los empleados y gerentes, y los riesgos de fallas en los procesos operativos de rutina (riesgo de los recursos humanos de la entidad, relacionado con la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo y apropiación de información sensible, entre otros).	• Falla en la no detección de cambios tecnológicos que hacen posible la detección de riesgos de soborno. • Falla en no planificar la adecuación de tecnología: necesidad de contar con mayores recursos económicos y/o modificaciones en la gestión del sistema, productividad, disminución de errores humanos, etc. • Fracaso en la implementación de nuevas tecnologías; crítico para lograr los objetivos anticorrupción. • Falta de control efectivo de TI. • Falla de seguridad de la información y otros problemas de seguridad.
Riesgos de seguridad cibernética (*cyber attacks*) - Factores internos: están relacionados con fallas en la seguridad y continuidad operativa de los sistemas informáticos, así como con problemas en su implementación o una inadecuada inversión en tecnología.	• Fallar en la seguridad informática al no detener/detectar fraudes, robo de identidad, extracción, destrucción, manipulación e intrusión de información sensible, crítica y confidencial que atente contra la integridad, de la organización y sus partes interesadas.

7.2 Identificar los riesgos (categorizaciones, eventos y sus causas)

Al planificar una evaluación del riesgo de corrupción en toda la organización, se debe prestar una atención cuidadosa a las partes interesadas involucradas en el proceso. Una variedad de partes interesadas podría contribuir a este ejercicio.

Dado que involucrar a más personas implicará más recursos y tiempo, esto también lleva a la pregunta de cómo se puede configurar el proceso de manera eficiente.

Esta sección explora los principios, técnicas y prácticas que pueden ayudar a una empresa a identificar categorizaciones, eventos, causas y consecuencias del riesgo, es decir:

¿Por qué ocurriría corrupción en la organización? y

¿Cómo se perpetraría la corrupción en la organización?

7.2.1 Recolección de datos

Hay diferentes formas de recopilar datos e información sobre por qué y cómo pueden ocurrir los riesgos de corrupción en una organización. Se presentan a continuación estos métodos y discutimos sus pros y contras.

Investigación de escritorio

La investigación de escritorio ofrece un excelente punto de partida para una evaluación de riesgos de corrupción. Deben considerarse tanto los recursos externos como los internos. Para ello, se puede utilizar los informes internos del departamento de Auditoría Interna sobre riesgos de cumplimiento, casos de incumplimiento y riesgos comunes de corrupción.

Otra fuente interna es analizando un registro de casos de corrupción pasados y las denuncias de irregularidades del canal de denuncias. Además, las verificaciones de antecedentes de terceros (por ejemplo, proveedores y agentes), los informes de diligencia debida de adquisiciones y las evaluaciones de los informes de licitación ofrecen una ventaja. También vale la pena considerar las fuentes externas que ofrecen perfiles de países sobre corrupción o casos de corrupción específicos de la industria.

Además de los informes fácilmente disponibles, una organización puede utilizar análisis adicionales usando datos financieros que brindan cifras de ventas y comisiones pagadas a los agentes para compilar una herramienta de análisis de sensibilidad de país/ubicación.

Asimismo, se podría considerar un análisis del gasto en entretenimiento, regalos y hospitalidad por unidad operativa. Las funciones de auditoría interna a menudo descargan datos relacionados con una unidad operativa en particular de los sistemas de TI y de contabilidad de toda la empresa para su análisis. Esto puede identificar áreas de mayor riesgo que pueden estar sujetas a una investigación más profunda empleando otros métodos. El mismo proceso se puede aplicar a la recopilación de datos relacionados con posibles riesgos de corrupción.

Por último, analizar los socios de negocio/terceras partes claves (partes externas con la que la organización tiene, o planifica establecer, algún tipo de relación comercial) en regiones de alto riesgo, además de las áreas en las que una empresa tiene interacciones con gobiernos o funcionarios gubernamentales; también puede ayudar a identificar dónde pueden existir riesgos de corrupción.

Entrevistas

Entrevistar a las partes interesadas clave puede ser un método eficaz para obtener una visión general de los riesgos de corrupción en una empresa. Primero, varias funciones corporativas del personal (tales como cumplimiento, legal, gestión de riesgos, auditoría interna, recursos humanos, contrataciones/compras, seguridad y cualquier unidad de investigación) pueden ofrecer información valiosa a un alto nivel.

La gerencia de línea que se ocupa de los riesgos operativos en el día a día a menudo puede proporcionar información adicional que surja de la experiencia operativa. Los dueños de ciertos procesos pueden identificar problemas específicos del proceso. También se podría considerar las opiniones de las partes interesadas externas (como los proveedores, los clientes, los auditores externos, los investigadores, las autoridades locales, los principales accionistas o inversores institucionales, e incluso los periodistas).

Las entrevistas pueden permitir más detalles que las encuestas o la investigación de escritorio y ofrecen la oportunidad de hacer preguntas adicionales, explorando los riesgos con más detalle. Las entrevistas pueden realizarse individualmente o en grupos pequeños siempre que no se excluyan las percepciones individuales debido a personalidades dominantes o dinámicas de grupo.

Encuestas y autoevaluaciones

Una encuesta puede ser una herramienta eficiente para recopilar opiniones sobre los riesgos de corrupción tanto de los empleados como de las partes externas. Las encuestas son una herramienta valiosa para recopilar opiniones de gerentes y empleados en diferentes funciones. Además de la identificación de los riesgos, la metodología de la encuesta también ayuda a crear conciencia sobre el tema de la corrupción. Las encuestas como herramienta por sí mismas presentan ventajas significativas, que incluyen:

- Bajo costo de implementación: dependiendo del modo de entrega, las encuestas pueden ser relativamente económicas de gestionar.
- Facilidad de implementación: la empresa tiene flexibilidad durante la fase de desarrollo para decidir cómo se debe administrar la encuesta, es decir, en línea, en persona, por correo electrónico, etc.
- Estandarización: las preguntas se pueden estandarizar para permitir uniformidad, lo que ayuda a medir e interpretar los resultados.

Una herramienta de autoevaluación es un recurso adicional para la identificación de riesgos, particularmente en empresas con diferentes ubicaciones y unidades operativas. Requiere que los riesgos sean identificados y compilados por personas relevantes dentro de la empresa para crear un registro de riesgos a partir de la información recibida. Uno de los muchos beneficios de una herramienta de autoevaluación es que proporciona un conjunto personalizado de riesgos de corrupción impulsados en gran medida por el conocimiento, la actitud y los procesos del entorno operativo de las empresas locales. Esto asegura que los entornos operativos de los segmentos clave de una empresa (como las unidades operativas) se consideren en lugar de desarrollar un conjunto de riesgos genéricos y estandarizados a nivel corporativo y trasladarlos a las unidades operativas.

Una encuesta se puede utilizar como una autoevaluación para la gerencia (divisional o regional) y también preguntando dónde ven riesgos de corrupción en sus operaciones

Al considerar una encuesta, una buena preparación es clave, ya que existen algunos conflictos potenciales:

- Conocimiento: el término "corrupción" se interpreta de manera diferente en todo el mundo. En algunos países, un obsequio comercial puede ser un acto de corrupción según las leyes penales aplicables, mientras que en otros países tal obsequio puede no entenderse como tal.
- Calidad de los datos: preguntarle a un gerente de un país cuáles son sus cinco riesgos principales de corrupción puede ser percibido por ese gerente como una expedición de "caza corporativa" que puede llevar a una solicitud no deseada de más controles y líneas jerárquicas. Esta percepción puede afectar las respuestas del gerente de ese país.
- Análisis: las preguntas abiertas pueden ser valiosas en algunas situaciones, pero a menudo conducen a un mayor trabajo en el análisis, potencialmente, en muchos idiomas diferentes.

Talleres, sesiones de lluvia de ideas o *focus group* (grupos focales)

El uso de talleres o sesiones de "lluvia de ideas" para explorar los riesgos de corrupción puede ser una forma eficaz y eficiente de recopilar opiniones de diferentes partes interesadas. Discutir las diferentes opiniones sobre los riesgos ayuda a generar comprensión.

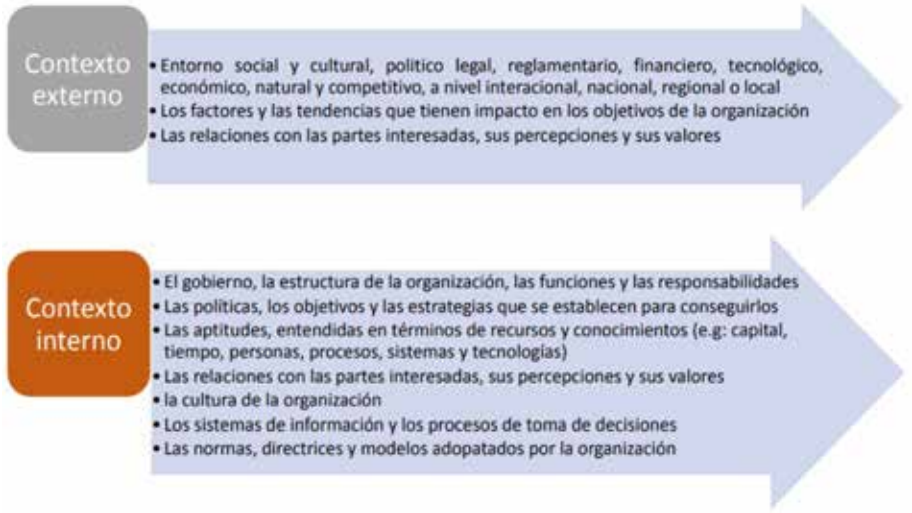
Un taller podría cubrir varios pasos en el proceso de evaluación de riesgos de corrupción. Podría comenzar, por ejemplo, en un formato de "sala de riesgos", llevando a los participantes a través de la etapa de definir y discutir los riesgos (categorizaciones y eventos), evaluar la probabilidad y el impacto potencial (causas y consecuencias) y dar como resultado un perfil de riesgo acordado y adaptado a la empresa.

Podría continuar y desarrollar un plan de acción para mitigar los riesgos. Una forma de identificar los posibles riesgos de corrupción podría ser plantear a cada participante la siguiente pregunta: "Si intentara ser corrupto, ¿Qué método utilizaría y cómo lo haría?".

Comprensión de la organización y su contexto

Análisis de los factores internos y externos

El análisis de los factores internos y externos es una de las consideraciones que debe incluir la revisión periódica por la alta dirección. Por ello, la organización deberá evidenciar, mediante informes, estudios, actas, y otro tipo de documentos la realización de este.



El análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) es uno de los más extendidos, dado que su orientación favorece la toma de decisiones estratégicas. Este análisis considera los factores internos (debilidades y fortalezas) y los factores externos (amenazas y oportunidades).

Ejemplo de matriz FODA

***Bow tie* análisis (BTA)**

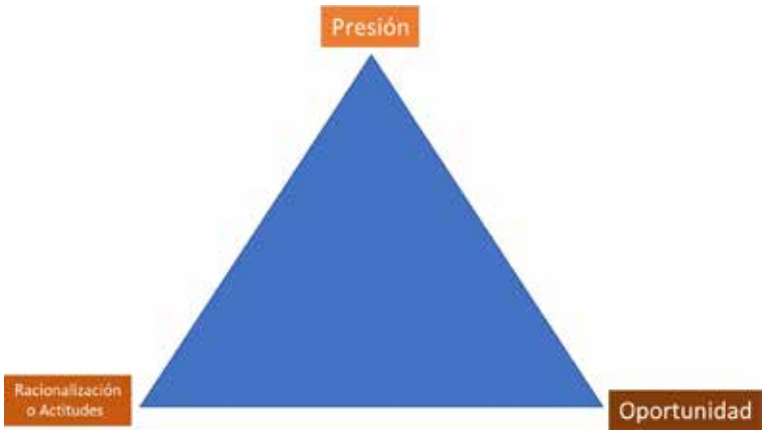
Este análisis es una forma esquemática de describir y analizar las vías de un riesgo desde las causas hasta las consecuencias, así como las debilidades de la gestión de riesgos. Combina el análisis de la causa del evento con sus consecuencias para prevenir o mitigar las consecuencias indeseables o estimular y promover las consecuencias deseables. A menudo es extraído directamente de una sesión de lluvia de ideas.

7.2.2 Identificar los riesgos

A continuación, definimos y brindamos ejemplos de categorizaciones, eventos y causas de riesgos de corrupción en procesos específicos.

Las categorizaciones, eventos y causas de riesgos son las razones por las que la corrupción puede ocurrir en una organización en función de su entorno, incluida la naturaleza y ubicaciones de sus operaciones. Una forma de ilustrar las categorizaciones, eventos y causas de riesgos es observar el *Fraud Triangle* (Triángulo del fraude) de *Donald Cressey*, que define tres elementos y condiciones que permiten que ocurra el fraude: presión/motivo, oportunidad y racionalización/actitudes. Aunque este triángulo se desarrolló en relación con los riesgos de fraude, también se puede usar para identificar las categorizaciones, eventos y causas de riesgos de corrupción. Al aplicar el *Fraud Triangle* para evaluar el riesgo de corrupción, se debe tener en cuenta los siguientes elementos:

- Una presión/motivo financiero o incentivo percibido (por ejemplo, presión para cumplir con las expectativas del cliente, objetivos financieros, objetivos de ventas).
- Una oportunidad percibida para cometer un acto de corrupción con baja probabilidad de detección (por ejemplo: monitoreo/controles que se perciben como ineficaces o una estructura corporativa muy compleja).
- Racionalización o actitudes (por ejemplo, historial de prácticas ilegales en la empresa, como que los competidores pagan sobornos, nadie se enterará, si no hago esto, perderé el contrato y mi trabajo, baja moral del personal).



Una vez que una empresa comprende las causas de los riesgos, puede identificar la consecuencia del riesgo dadas esas categorizaciones y eventos. Estos eventos de riesgo representarían ejemplos de dónde y cómo puede ocurrir la corrupción en la empresa.

Para realizar una evaluación exhaustiva del riesgo de corrupción, es útil distinguir entre "categorizaciones de riesgos de corrupción", "eventos de esas categorizaciones" y "las causas y consecuencias de la corrupción".

7.2.3 Riesgos de corrupción en procesos específicos

A continuación, se presentan algunos ejemplos de procesos específicos que son vulnerables a la corrupción y merecen atención adicional al realizar una evaluación de riesgos de corrupción para una organización.

Adquisiciones

Para la mayoría de las empresas, la función de contrataciones o abastecimiento es crucial para su negocio.

Al comprar productos o servicios de los proveedores, especialmente cuando el proveedor depende en gran medida del contrato, existen algunos riesgos de corrupción comunes que deben tener en cuenta:

Sobornos y comisiones ilegales

Los empleados en la función de abastecimiento (o sus gerentes) pueden recibir un soborno o comisión ilegal por parte del proveedor a cambio de obtener negocios. Este soborno puede ser en efectivo o puede involucrar cualquier cosa de valor, como: obsequios, viajes, comidas y entretenimiento no estándar, uso de tarjetas de crédito o transferencias de efectivo disfrazadas de "préstamos". Pero los empleados de abastecimiento también podrían solicitar un soborno, por ejemplo, ofreciéndose a aceptar pagar un precio superior por bienes o servicios a cambio.

Esquemas de sobrefacturación

La sobrefacturación es un esquema de fraude financiero mediante el cual una empresa recibe precios de factura más altos de lo normal, que se pagarán porque la persona que aprueba las facturas está involucrada en el esquema. Es posible que el aprobador de facturas ya haya recibido un soborno o que al proveedor simplemente se lo esté utilizando como un vehículo para transferir efectivo que finalmente se reembolsará a los oficiales de adquisiciones.

Manipulación de licitaciones y fijación de precios

Durante situaciones de oferta/propuesta/licitación, varios proveedores pueden unir fuerzas y comprometer el proceso de licitación al acordar quién ofrecerá el precio más bajo para ganar el proyecto. A cambio, los otros proveedores que participan en el esquema de manipulación de licitaciones ofrecerán el precio más bajo en situaciones de licitación para otros proyectos.

Este riesgo aumenta cuando solo hay unos pocos proveedores que pueden brindar el servicio (es decir, un oligopolio en un sector altamente especializado) o cuando el proyecto es costoso y el proveedor debe hacer una inversión considerable para ganar el proyecto (por ejemplo, para grandes proyectos de infraestructura).

Ventas

Los esquemas mencionados en la sección "Adquisiciones" anterior también podrían aplicarse a los procesos de ventas. Además, se debe considerar algunos de los siguientes riesgos de corrupción:

Uso de agentes

Al ingresar a nuevos mercados, las empresas a menudo dependen de agentes o consultores para familiarizar a la empresa con una nueva región y las prácticas comerciales locales, o para presentar la empresa a clientes potenciales. Por lo general, el agente trabaja a comisión y recibe un porcentaje de las ventas como tarifa. A veces, los agentes aseguran los contratos compartiendo sus honorarios con el personal del lado del cliente.

Regalos y entretenimiento lujosos

Los obsequios, comidas y entretenimientos habituales se consideran aceptables en muchos países. Las diferencias culturales hacen que a veces sea difícil decidir qué es lo correcto.

Se puede esperar que los gerentes de ventas entreguen obsequios personales exclusivos que pueden ser costosos o que paguen cenas de negocios y entretenimiento nocturno. Esta situación puede convertirse fácilmente en una pendiente sinuosa, lo que dificulta evitar pagos que cruzan la línea entre las prácticas permisibles y el soborno. Cuando la empresa no está al tanto de las costumbres locales, la competencia es feroz o se involucran oportunidades comerciales importantes, la empresa puede sentirse presionada para aceptar la situación y participar en prácticas que violan las leyes o regulaciones en una o más jurisdicciones.

Importación y exportación de mercancías - pagos por despacho de aduana o transporte de mercancías

Al importar o exportar bienes, los funcionarios de la aduana pueden solicitar un soborno (o ayudar a los clientes que ofrecen sobornos primero). Especialmente cuando hay presión de tiempo para acelerar el despacho (productos perecederos, multas por entrega tardía, etc.), el funcionario de aduanas podría aprovechar la situación.

Cuando se transportan mercancías en determinadas geografías, los funcionarios locales pueden exigir una tarifa para permitir que los vehículos que transportan las mercancías o el personal de la empresa utilicen una ruta determinada o pasen un puesto de control, incluso si todas las visas o permisos oficiales están en regla.

Dichos pagos son comunes en muchos países, aunque pueden estar prohibidos por ley o reglamento para que el pagador los ofrezca o realice, o el beneficiario los solicite o reciba.

Interacción con el gobierno

Hacer negocios a menudo implica la interacción con el gobierno. Ejemplos de interacciones con entidades o funcionarios gubernamentales incluyen tener un cliente de gobierno y un socio de gobierno, tratar con funcionarios de aduanas y obtener permisos, visas o licencias (por ejemplo, para formar una entidad legal; realizar negocios; producir, importar, transportar o entregar ciertos bienes y servicios; construir una instalación de producción u otras instalaciones; poseer u operar un vehículo; contratar personal local o extranjero; o hacer que el personal extranjero de la empresa resida y trabaje en el país, etc.).

Cuando el permiso, visa o licencia es crítico y una empresa no tiene alternativas, el riesgo de soborno, comisiones ilegales o extorsión es común en ciertos lugares.

Apoyo político

En algunos países, los funcionarios del gobierno nacional o local pueden solicitar una contribución "voluntaria" a un partido político una vez que se otorga un permiso o se otorga un proyecto de construcción. Aunque no es necesariamente ilegal según las leyes locales, esto podría interpretarse como un pago indebido en violación de las leyes de soborno en el extranjero de muchos países.

Protocolos de seguridad

En ciertos países, es posible que se requiera que una empresa tenga seguridad en el país para sus empleados en respuesta a los riesgos de seguridad planteados en ciertos países. La fuerza policial local que está obligada por ley a proporcionar dicho servicio puede solicitar sobornos por encima de la tarifa estipulada por el gobierno regular.

Además, las empresas de seguridad pueden poner en riesgo a una entidad si esa empresa de seguridad actúa de manera poco ética o viola las leyes de corrupción mientras actúa en nombre de una empresa.

Programas sociales

Pueden surgir otras situaciones en las que los funcionarios del gobierno presionen a las empresas/contratistas para que ayuden con proyectos de infraestructura local o programas sociales, que están directamente afiliados a ciertos políticos, partidos políticos o sus intereses.

Contribuciones benéficas y patrocinios

Las contribuciones caritativas y el patrocinio de eventos y conferencias también pueden presentar riesgos para sobornos. Las contribuciones a organizaciones benéficas que estén realmente vinculadas a actividades corruptas, o que sean vehículos clandestinos de lavado de dinero pueden exponer potencialmente a una empresa a violaciones de las leyes de corrupción en ciertos países. El patrocinio de conferencias organizadas o a las que asisten entidades o funcionarios gubernamentales también puede exponer potencialmente a una empresa a violaciones de las leyes de corrupción en ciertos países.

Riesgos de la industria

Si bien algunos riesgos de corrupción pueden aplicarse a muchas o todas las industrias, otros pueden ser más específicos de la industria. Como se discutió en la "Evaluación de riesgos de corrupción", dependiendo de los sectores industriales en los que o con los que la empresa realiza negocios, la probabilidad de que la corrupción se convierta en incidentes reales de corrupción puede variar considerablemente.

7.2.4 Elementos para incluir en el Registro de riesgos (EB)

Cada categoría, sus eventos de riesgo y causa de riesgo podrían documentarse individualmente en el Registro de riesgos.

Veamos a continuación un ejemplo de cómo documentar tres categorías riesgos de corrupción (Riesgo estratégico, Riesgo de Integridad y Riesgo relacionado con Socios de Negocio/Terceras partes) y sus eventos asociados, causas y consecuencias de la falla en el Registro de riesgos.

Ubicación/Región			
Unidad de Negocio: Unidad XYZ			
Categoría de riesgo de corrupción	**Riesgo estratégico**	**Riesgos de Integridad**	**Riesgos relacionados con Socios de Negocio**
Evento del riesgo de corrupción	No proporcionar un alto nivel de integridad, transparencia y fiabilidad del servicio, y la entrega de productos; y garantizar una mejora continua.	No impedir el soborno a un funcionario con el objetivo de facilitar la expedición de licencias, permisos, certificados y otros tipos de servicios públicos.	Fallar en asegurar la participación de los socios de negocio a la política de tolerancia cero al soborno y la corrupción de la entidad.
Consecuencias de la falla	Financieros, legales, regulatorios, operativos y de reputación.	Financieros, legales, regulatorios, operativos y de reputación.	Daño del patrimonio institucional, daño de la imagen y reputación.
Causa de la falla	Fallar en el compromiso estratégico del liderazgo.	Fallar en la toma de conciencia y formación.	Falta de difusión de la cultura corporativa.

7.3 Calificación de la probabilidad y el impacto potencial de cada evento de corrupción (EB)

Asignar recursos de manera eficiente y efectiva para los riesgos de corrupción identificados en cada evento es calificar la probabilidad de que pueda ocurrir y el impacto potencial correspondiente de ese suceso. El objetivo es priorizar las respuestas a estos riesgos de corrupción en un formato lógico basado en una combinación de su probabilidad de ocurrencia y su impacto potencial.

Existe cierta subjetividad en la evaluación de la probabilidad y el impacto potencial, y las calificaciones se verán influenciadas por la experiencia y los antecedentes de los miembros del equipo de evaluación. En ocasiones, la evaluación puede reflejar un punto de vista dominante o un nivel de sesgo, consciente o inconsciente, que hace que los resultados no sean creíbles para un tercero objetivo o un especialista en lucha contra la corrupción. Entonces puede ser necesaria la intervención de un facilitador, cuyo objetivo es ayudar a evitar invertir mucho tiempo y esfuerzo en una evaluación sin lograr resultados válidos.

7.3.1 Calificación de probabilidad de ocurrencia

La probabilidad de cada evento de riesgo identificado debe evaluarse sin considerar las medidas de mitigación en la organización.

La gerencia debe considerar la probabilidad de que el evento de riesgo sea perpetrado por un individuo o grupo de individuos que actúan de manera colusoria. Bajo este marco, se recomienda que la evaluación de la probabilidad se exprese como la probabilidad de que el evento ocurra dentro de los próximos 12 meses. Este plazo debe ajustarse según sea necesario para adaptarse a las características de los objetivos de gestión del riesgo de corrupción de la empresa.

Algunas de las causas a considerar al estimar la probabilidad de cada evento de riesgo de corrupción incluyen:

- La naturaleza de la transacción o proceso con el que se relaciona el evento (por ejemplo, si existe alguna interacción con funcionarios gubernamentales).
- Incidentes del evento de riesgo de corrupción ocurridos en el pasado en la empresa.
- Incidentes del evento de riesgo de corrupción en la industria empresarial.
- La cultura y el ambiente de corrupción local en la región donde se perpetraría el evento.
- El número de transacciones individuales relacionadas con el evento.
- La complejidad del evento de riesgo, el nivel de conocimiento y habilidad requeridos para su ejecución.
- El número de personas necesarias para llevar a cabo el plan.
- El número de personas involucradas en la aprobación o revisión del proceso o transacción relacionada con el evento.

Para empresas con múltiples ubicaciones y unidades operativas, la probabilidad de cada evento de riesgo de corrupción puede variar entre diferentes ubicaciones y unidades operativas. Por ejemplo, el soborno de un funcionario gubernamental para el despacho de aduanas puede ser más probable en ciertos países y menos probable en otros.

7.3.2 Calificación del impacto potencial de la ocurrencia

El proceso de evaluación del impacto potencial de un evento de riesgo se lleva a cabo de manera similar al proceso de probabilidad. El equipo de evaluación debe evaluar la magnitud del impacto po-

tencial de cada evento de riesgo en particular. Por lo general, esta consideración del impacto potencial cubre una amplia gama que incluye daños financieros, legales, regulatorios, operativos y de reputación.

Algunas de las consecuencias a considerar al estimar el impacto potencial de cada evento de riesgo incluyen:

- Impacto de incidentes pasados de riesgos de corrupción en la empresa si los hubiere.
- Impacto de los incidentes del evento de corrupción en otras empresas.
- Cantidades potenciales de multas o sanciones.
- El costo de oportunidad que surge de las restricciones reglamentarias sobre la capacidad de la empresa para operar o expandirse.
- Impacto en operaciones, como la interrupción de la capacidad de la empresa para transportar mercancías u obtener permisos u otras aprobaciones requeridas.
- Impacto potencial en los estados financieros.
- Impacto en la contratación y retención de empleados.
- Impacto en la retención de clientes e ingresos futuros.
- Impacto financiero de costos de litigio.
- Impacto reputacional.

Para empresas con múltiples ubicaciones o unidades operativas, el impacto potencial de cada evento puede variar entre diferentes ubicaciones y unidades de negocio. Por ejemplo, algunas unidades operativas en una empresa comercial pueden vender bienes de pequeño valor a consumidores individuales que se compran en tiendas minoristas, mientras que otra unidad de negocios puede vender bienes de valor mayor o total a instituciones, incluidos los gobiernos.

7.3.3 Métodos de calificación

Hay muchas formas diferentes de calificar y comunicar la probabilidad o el impacto potencial de cada evento de riesgo de corrupción. Se podría utilizar una escala cuantitativa, con puntuaciones aplicadas juiciosamente a cada evento de riesgo. En la tabla de "Ejemplo de Matriz de puntaje de probabilidad" y "Ejemplo de Matriz de puntuación de impacto potencial" se ilustran ejemplos de matrices de puntuación de cinco puntos.

Ejemplo de Matriz de puntaje de probabilidad

Matriz de puntuación de cinco puntos para evento de riesgo de corrupción identificado
1 - MUY IMPROBABLE - Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 25% de seguridad de que este se materialice.
2 - IMPROBABLE - Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 25% a 50% de seguridad de que este se materialice.
3 – MODERADA - Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 51% a 74% de seguridad de que este se materialice.
4 - PROBABLE - Alta - Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 75% a 89% de seguridad de que este se materialice.
5 - CASI CERTEZA - Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene plena seguridad de que este se materialice; tiende a estar entre 90% y 100%.

Ejemplo de Matriz de puntaje de impacto potencial

Ejemplo de Matriz de puntuación de impacto potencial de cinco puntos para evento de riesgo de corrupción identificado	Puntaje
INSIGNIFICANTE - Riesgo cuya materialización puede generar pérdidas financieras que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la organización.	**1**
MENOR - Afecta parcialmente al proceso. Riesgo cuya materialización puede generar pérdidas financieras que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la institución.	**2**
MODERADO - Afecta parcialmente al proceso. Riesgo cuya materialización puede generar pérdidas financieras que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la institución.	**3**
MAYOR - Impacto negativo en la Institución. Riesgo cuya materialización puede generar pérdidas financieras que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la institución.	**4**
CATASTRÓFICO - Consecuencias desastrosas sobre el sector. Riesgo cuya materialización puede dar lugar a la finalización de la actividad de la institución, pérdidas reputacionales, de imagen y consecuencias legales.	**5**

Algunas empresas, en particular las que son más grandes y pueden asignar recursos apropiados para este ejercicio, pueden preferir incluir más criterios para sus matrices de puntuación. Como alternativa a la matriz anterior, otra opción puede ser incluir definiciones de ciertos factores para proporcionar más estructura a quienes evalúan las calificaciones. En la probabilidad de calificación, estos factores podrían incluir el porcentaje de probabilidad de ocurrencia, el estado de los casos reales y la complejidad del evento de riesgo. Al calificar el impacto potencial, podrían incluir el impacto en la reputación, el impacto financiero, el impacto regulatorio, el impacto en los clientes y el impacto en los empleados. Se presentan más abajo las Tablas de "Ejemplo de Matriz de puntaje de probabilidad multifactorial" y "Ejemplo de Matriz de puntaje de impacto potencial multifactorial" para ver ejemplos de estos enfoques.

Ejemplo de Matriz de puntaje de probabilidad multifactorial

Probabilidad	Puntaje	Cuantitativo	Estado de los casos reales del evento de riesgo	Complejidad
Muy baja probabilidad de actividad de corrupción.	1	<10% de probabilidad	Se ha corregido la causa raíz del incidente (reduciendo la posibilidad de que se repita).	Muy difícil de perpetrar incluso sin lugar de controles.
Poca probabilidad de actividad de corrupción.	2	10%–25% de probabilidad	La causa principal del incidente está en proceso de ser remediada.	Difícil de perpetrar incluso sin controles en su lugar.

Probabilidad	Puntaje	Cuantitativo	Estado de los casos reales del evento de riesgo	Complejidad
Alguna probabilidad de actividad de corrupción.	3	26%–50% de probabilidad	Se ha contenido el incidente.	Moderadamente complejo de perpetrar sin controles en su lugar.
Probabilidad considerable de actividad de corrupción.	4	51%–75% de probabilidad	El incidente está en proceso de ser contenido.	Fácil de perpetrar sin controles en su lugar.
Muy alta probabilidad de actividad de corrupción.	5	> 75% de probabilidad	El incidente ha sido reportado y actualmente está bajo investigación.	Muy fácil de perpetrar sin controles en su lugar.

Ejemplo de Matriz de puntuación de impacto potencial multifactorial

Impacto potencial	Puntaje	Reputación	Financiero	Legal/ Cumplimiento	Partes interesadas/ Clientes	Partes interesadas/ Empleados
Impacto no significativo	1	Mínima atención de los medios locales rápidamente contenida, recuperabilidad a corto plazo.	El impacto financiero es <5% de la partida presupuestaria seleccionada (por ejemplo, facturación o ingresos).	Aviso de infracción / advertencias que requieran acción administrativa y sanciones mínimas.	Quejas mínimas de clientes y costos de recuperación.	Impacto insignificante en la capacidad del Departamento de ___ para contratar y retener empleados.
Impacto menor	2	Impacto del mercado local en la marca y la reputación del Departamento.	El impacto financiero está entre el 5% y el 10% de la partida presupuestaria seleccionada (por ejemplo, facturación o ingresos).	Los litigios de los órganos de gobierno sujetos a multas y sanciones moderadas pueden estar sujetos a procedimientos regulatorios y / o audiencias.	Disminución mínima en las relaciones con los clientes y algunos costos de recuperación.	Algún impacto en la capacidad del ___ Departamento para contratar y retener empleados.

Impacto potencial	Puntaje	Reputación	Financiero	Legal/ Cumplimiento	Partes interesadas/ Clientes	Partes interesadas/ Empleados
Impacto moderado	3	Cobertura sostenida de la prensa local con implicaciones cada vez mayores para los clientes.	El impacto financiero está entre el 10% y el 20% de la partida presupuestaria seleccionada (por ejemplo, facturación o ingresos).	Litigios sujetos a multas o sanciones sustanciales, sujetos a procedimientos regulatorios y / o audiencias.	Pérdida o deterioro de las relaciones con los clientes y costos de recuperación moderados.	Impacto significativo en la capacidad del Departamento de ---- para contratar y retener a los mejores.
Impacto mayor	4	Cobertura de prensa nacional o regional sostenida con daño a largo plazo a la imagen pública.	El impacto financiero está entre el 20% y el 30% de la partida presupuestaria seleccionada (por ejemplo, facturación o ingresos).	Potencialmente, un escrutinio significativo del órgano de gobierno, investigaciones sujetas a multas y sanciones sustanciales, que pueden incluir algunos cargos penales, sujetos a procedimientos regulatorios y / o audiencias.	Relaciones tensas con los clientes clave y costos de recuperación significativos y amenaza para el crecimiento futuro.	Gran impacto en la capacidad del Departamento de ---- para contratar a los mejores.
Impacto catastrófico	5	Cobertura global de los medios.	El impacto financiero está > 30% de la partida presupuestaria seleccionada (por ejemplo, ingresos o egresos).	Gran escrutinio, investigaciones sujetas a multas y sanciones sustanciales, incluidos cargos penales y/u órdenes de cese y desistimiento, posible acción reguladora.	Pérdida de relaciones importantes con los clientes y grave amenaza para el crecimiento futuro.	Impacto sostenido en la capacidad del Departamento de ___ para contratar y retener a los mejores.

7.3.4 Cálculo del riesgo inherente

La combinación de las evaluaciones de impacto potencial y de probabilidad para cada evento de riesgo de corrupción da como resultado una evaluación del riesgo de corrupción inherente. El riesgo inherente representa el nivel de riesgo general de cada evento sin tener en cuenta las medidas de mitigación. Son estas áreas donde la mitigación de los controles probablemente será más importante para mitigar los eventos de corrupción.

Hay muchas formas diferentes de determinar el riesgo inherente de cada evento de riesgo de corrupción. El riesgo inherente se puede determinar cuantitativamente como un factor de las evaluaciones de probabilidad y de impacto potencial.

Como ejemplo de una escala cuantitativa simple, consulte los formatos de puntuación en las Tablas de “Ejemplo de Matriz de puntaje de probabilidad” y “Ejemplo de Matriz de puntuación de impacto po-

tencial" en **Métodos de calificación**, donde cada riesgo de corrupción identificado tiene una puntuación de probabilidad numérica y una puntuación de impacto potencial numérica. La multiplicación de estas dos puntuaciones se puede utilizar para calcular un puntaje de riesgo inherente.

Puntaje de probabilidad de riesgo de corrupción	**A**
x	
Puntuación del impacto del riesgo de corrupción potencial	**B**
Puntuación de riesgo inherente	**C**

Utilizando la escala cuantitativa de 1 a 5 de las Tablas de "Ejemplo de Matriz de puntaje de probabilidad" y "Ejemplo de Matriz de puntuación de impacto potencial" en **Métodos de calificación**, en la Tabla de "Ejemplo de enfoque cuantitativo para evaluar el riesgo inherente" se incluye un ejemplo de cómo se puede determinar cuantitativamente el riesgo inherente.

Ejemplo de enfoque cuantitativo para evaluar el riesgo inherente

Nivel de Riesgo Inherente	Multiplicación de los puntajes de probabilidad y de impacto potencial
Aceptable	4 o menos
Moderado	5 - 6
Importante	8 - 12
Inaceptable	15-25

7.3.5 Cisnes negros, evaluaciones de riesgos y el impacto de la ignorancia

Los "cisnes negros" (Taleb, 2007) son acontecimientos que se cree que están fuera de lo posible y, sin embargo, ocurren. Los percibimos como sucesos aleatorios, pero esconden trampas lógicas que nos impiden la visión de conjunto. A estos sucesos aparentemente aleatorios, que a menudo tienen profundas consecuencias para el individuo e incluso para las sociedades en su conjunto, Taleb los llama "Cisnes Negros". Ocurren cuando nuestro juicio se ve nublado por el deseo de encajar la información en narrativas ordenadas y fáciles de entender. Se parecen mucho a los actos de corrupción que, en opinión de la Alta Dirección, jamás podrían ocurrir en una empresa con tantos controles.

Como seres humanos, somos especialmente buenos a la hora de convertir todos los estímulos de nuestro entorno en información significativa, pero que seamos capaces de reflexionar y ordenar el mundo que nos rodea no significa necesariamente que lo hagamos siempre bien. Para empezar, tendemos a tener una mirada estrecha sobre nuestras creencias: una vez que tenemos una idea sobre cómo funciona el mundo, nos aferrarnos a ella. Pero, como el conocimiento humano está en constante crecimiento y evolución, este enfoque dogmático tiene poco sentido.

Este tipo de pensamiento dogmático puede dar lugar a grandes sorpresas. A veces nos sorprenden los acontecimientos no porque sean aleatorios, sino porque nuestra perspectiva es demasiado estrecha. Estos "Cisnes Negros" pueden llevarnos a reconsiderar radicalmente nuestra visión del mundo. Serán tan triviales como aprender que no todos los cisnes son blancos, o tan transformadores como advertir que alguien de la Alta Dirección paga sobornos o acepta de clientes a personas vinculadas al narcotráfico. Cada escándalo de Compliance que vemos casi a diario en las noticias esconde un Cisne Negro.

El efecto de un "Cisne Negro" no es el mismo para todos. Algunos se verán enormemente afectados, otros, apenas. La potencia de su efecto viene determinada en gran medida por el acceso a la información pertinente: cuanta más información se tenga, menos probabilidades de verse afectado por un Cisne Negro; y cuanto más ignorante se sea, más riesgo se corre.

7.3.6 Determinantes de los riesgos para el análisis de causas y cálculo de probabilidades.

Entender los determinantes de los riesgos (Preve, 2014) permite identificar sus causas. Significa comprender las razones o circunstancias que aumentan su probabilidad de ocurrencia. Podemos afirmar, dice Preve, que un factor de riesgo es una función de sus determinantes:

Riesgo: fx (determinantes del riesgo)

La medición de la probabilidad, cuando se basa en datos del pasado, no solo es poco útil, sino que además puede resultar hasta cierto punto engañosa, creando una falsa sensación de certeza. Lo que importa son las razones por las que una variable (el riesgo de pagar una coima, por ejemplo) se comporta de tal o cual forma, o la razón por la que se produce el evento: necesitamos conocer los determinantes. No siempre son los mismos y tienden a cambiar a lo largo del tiempo de una situación a otra.

En materia de Compliance, típicamente surgen para cada riesgo varios determinantes. Los determinantes más importantes y a la vez más difíciles de encontrar y describir son los relacionados con la cultura: la presión por resultados; el *Tone at the Top* (y en el medio); la consistencia de los valores con los incentivos; la justicia interna; el clima de transparencia, así como el rol y la posición del Compliance *Officer*, las políticas y procesos, el entrenamiento y la comunicación (Kleinhempel, 2021).

En la misma línea, Kaplan complementa la lista de determinantes relacionados con la cultura de Compliance (Kaplan, 2019):

- Pensamiento demasiado cortoplacista.
- Escasa identificación de los empleados con la empresa, sus clientes o sus productos/servicios.
- Otros indicios de "riesgo moral" (desajuste de incentivos y riesgos).
- Dificultad para plantear preguntas/preocupaciones (no solo las de Compliance).
- Sensación de injusticia o preocupación por la falta de "justicia organizativa".
- Tono directivo cuestionable no solo en "Top", sino también en el "Middle" y en los "bordes".
- Marginación de las preocupaciones de los colaboradores sobre asuntos de Compliance.
- Presión irrazonable sobre la performance individual y grupal.
- Recompensa de la mala conducta mediante ascensos, indemnizaciones, etc.

¿Por qué la cultura? En el mundo de Compliance hay consenso sobre la necesidad de incluir una dimensión cultural en la evaluación de riesgos, siendo su principal determinante. Sin embargo, la importancia de hacerlo puede ser menos evidente para otras personas de una empresa. Y los lineamientos y las guías emitidos al respecto tampoco ayudan demasiado, al punto que los determinantes culturales se abordan tangencialmente o se omiten por completo. La reciente guía de GAFILAT[3] dirigida al sector de Actividades y Profesiones No Financieras Designadas (APNFD)[4] para la construcción de una matriz de riesgos en prevención del LA/FT cita ejemplos de causas/vulnerabilidades relacionadas con los factores de riesgo, pero no se incluye ninguno de los determinantes que citan Kaplan y Kleinhempel. No obstan-

[3] GAFILAT recomienda utilizar una fórmula de redacción para eventos de riesgo con tres elementos: amenazas (factor externo) + vulnerabilidad (factor interno) + consecuencia o impacto (¿qué?). Entendemos que la vulnerabilidad interna es compatible con el concepto de determinantes de los riesgos, en el sentido que le damos en este documento. GAFILAT, además, aporta algunas recomendaciones interesantes para la redacción de los eventos de riesgo:

▪ Redacte de forma clara, específica y directa, sin dar lugar a ambigüedades.

▪ Procure evitar calificativos como "malo" o "poco"; prefiera otros más precisos como "deficiente", "insuficiente" o "ineficiente".

▪ No inicie la redacción con expresiones como "falta de…" u otras frases similares que llevan implícito el sesgo hacia una supuesta solución particular.

[4] El Grupo de Acción Financiera (GAFI) ha determinado como sujetos obligados a cinco categorías de Actividades y Profesiones No Financieras Designadas (APNFD): a) casinos; b) agentes inmobiliarios; c) comerciantes de piedras preciosas y comerciantes de metales preciosos; d) notarios, abogados, otros profesionales jurídicos independientes y contadores ; y e) los proveedores de servicios fiduciarios y societarios, que están "especialmente expuestos al riesgo de lavado de fondos y financiamiento del terrorismo" (GAFILAT, 2021).

te, enfatiza la importancia de establecer las posibles causas de los eventos de riesgo. Esto es sumamente importante porque permite identificar las situaciones que podrían favorecer la materialización de cada evento de riesgo (GAFILAT, 2021).

En las guías para evaluación de riesgos de corrupción tampoco encontramos los determinantes culturales tratados de manera explícita, sino que los ejemplos gravitan principalmente sobre determinantes externos a la organización o relacionados con la naturaleza de las transacciones[5].

Cuando los riesgos se materializan por conductas impropias, ¿qué tipo de incentivos, compensaciones y sistemas de control generan que se haga lo correcto? Pensar detenidamente en los incentivos y diseñar sistemas que los alineen suele ser la parte más sensible de la cultura corporativa. Hacia allí se dirigen, en sus aspectos sustantivos, los últimos ajustes a la guía del Departamento de Justicia de los EE.UU. (DoJ) para evaluar la efectividad de los programas de Compliance[6]. Los incentivos de la Alta Dirección deberían ser una parte central en el ámbito de la gestión de riesgos de Compliance, por cuanto representan el principal determinante de la ocurrencia de los eventos que se buscaba prevenir.

¿Quién debería participar en los cálculos de riesgo inherente?

Una de las claves para un proceso de evaluación eficaz de riesgos es tener a las personas adecuadas que califiquen la probabilidad y el impacto potencial de cada evento de riesgo de corrupción. Es importante involucrar solo a aquellas personas que están familiarizadas con la transacción o el proceso afectado por cada evento, incluidos los dueños del proceso.

En los casos en que se busquen las opiniones de más de una persona, se podría tomar un promedio de la puntuación. Involucrar a varias personas (cada una responsable de áreas relevantes para ellos) puede ayudar a reducir el efecto de los sesgos individuales que de otro modo podrían sesgar los resultados.

Una de las funciones del dueño de la evaluación de riesgos de corrupción podría ser evaluar la razonabilidad de las puntuaciones brutas designadas por las partes relevantes y hacer sugerencias para cuestionar o revaluar cualquier puntuación que parezca cuestionable. Los protocolos para estimar las calificaciones (incluido quién debería estar involucrado) y cuestionar o proponer cualquier reevaluación de las calificaciones deben determinarse preferiblemente por adelantado como parte del procedimiento general de evaluación de riesgos de corrupción. Esto puede ayudar a evitar que una o más personas anulen de manera inapropiada los juicios de las personas más cercanas a los riesgos en un intento de producir un resultado que sea más conveniente que preciso.

¿Cuándo y cómo realizar cálculos de riesgo inherente?

El proceso para determinar el nivel de riesgo inherente se puede realizar al mismo tiempo que la identificación de los eventos discutidos en la sección anterior o como un paso separado.

---

[5] Algunos de los factores a tener en cuenta a la hora de estimar la probabilidad de cada trama de corrupción son (United Nations Global Compact, 2013):
- La naturaleza de la transacción o el proceso al que se refiere el evento (por ejemplo, si hay alguna interacción con funcionarios públicos).
- Incidentes de corrupción ocurridos en el pasado en la empresa.
- Incidentes de corrupción en el sector de la empresa.
- La cultura y el entorno locales de corrupción en la región en la que se perpetraría el evento.
- El número de transacciones individuales relacionadas con el evento.
- La complejidad del evento y el nivel de conocimientos y habilidades necesarios para su ejecución.
- El número de individuos necesarios para perpetrar el evento.
- El número de personas implicadas en la aprobación o revisión del proceso o transacción relacionados con el evento.

[6] El 2 y 3 de marzo de 2023, durante los discursos de la Fiscal General Adjunta (DAG) Lisa Monaco y el Fiscal General Adjunto (AAG) Kenneth A. Polite, Jr., en el *38th National Institute on White Collar Crime* de la ABA en Miami, el Departamento de Justicia de EE. UU. (DoJ) *Criminal Division* anunció varias actualizaciones de políticas consistentes con las iniciativas anunciadas en el Memorando de Mónaco de septiembre de 2022. Específicamente, el DoJ publicó, entre otros, la Guía actualizada sobre la "Evaluación de los Programas de Cumplimiento Corporativo".

Independientemente, las calificaciones de riesgo inherente deben discutirse después de que se hayan identificado todos los eventos para que no obstaculicen el proceso de identificación de riesgos.

Hay varios enfoques organizativos para evaluar los riesgos inherentes. Una es realizar talleres o reuniones grupales, ya sea para las funciones relevantes o para los individuos que serán responsables de las calificaciones preliminares de probabilidad y potencial impacto para un grupo de eventos.

Durante estas sesiones, se les puede pedir a los participantes que califiquen cada evento de riesgo de forma anónima o abierta. Esto se puede hacer discutiendo cada evento de riesgo para llegar a una calificación de consenso, o haciendo que cada participante califique individualmente cada evento (ya sea de manera abierta o anónima) y luego calculando la puntuación promedio del grupo para cada evento de riesgo.

Otro enfoque es utilizar encuestas *on line*, donde se les pide a los participantes que proporcionen una calificación para cada evento de riesgo a través de una intranet o correo electrónico. Para esta opción, se debe asignar una persona para coordinar la encuesta y recopilar los resultados. Una tercera opción es que la persona responsable de coordinar la evaluación de riesgos se reúna con cada participante, obtenga sus puntajes y luego calcule un puntaje de riesgo inherente promedio para cada evento. Una cuarta opción es que la persona responsable de la evaluación de riesgos realice una evaluación preliminar de las calificaciones de riesgo por sí misma y luego la proporcione a los dueños y funciones del proceso relevantes para que la revisen y enmienden si es necesario. Un peligro de este último enfoque es que las puntuaciones iniciales proporcionadas pueden sesgar las respuestas de los participantes y conducir a un resultado que sea un reflejo de la opinión de una persona.

Inclusión de calificaciones de riesgo inherentes en el registro de riesgos

La probabilidad asignada general, el impacto potencial y las calificaciones de riesgo inherente para cada evento se pueden incluir en el Registro de riesgos de la siguiente manera:

Ubicación/Región			
Unidad de Negocio: Unidad XYZ			
Categoría de riesgo de corrupción	**Riesgo estratégico**	**Riesgos de Integridad**	**Riesgos relacionados con Socios de Negocio**
Evento del riesgo de corrupción	No proporcionar un alto nivel de integridad, transparencia y fiabilidad del servicio y la entrega de productos y garantizar una mejora continua.	No impedir el soborno a un funcionario con el objetivo de facilitar la expedición de licencias, permisos, certificados y otros tipos de servicios públicos.	Fallar en asegurar la participación de los socios de negocio a la política de tolerancia cero al soborno y la corrupción de la entidad.
Consecuencias de la falla	Financieros, legales, regulatorios, operativos y de reputación.	Financieros, legales, regulatorios, operativos y de reputación.	Daño del patrimonio institucional, daño de la imagen y reputación.
Causa de la falla	Fallar en el compromiso estratégico del liderazgo.	Fallar en la toma de conciencia y formación.	Falta de difusión de la cultura corporativa.
Probabilidad	2	3	1
Impacto potencial	4	5	3
Riesgo inherente	**8 Importante**	**15 Inaceptable**	**3 Aceptable**

7.4 Identificación de acciones de mitigación, controles y procesos (EB)

Los controles para prevención de la corrupción son únicos, ya que van mucho más allá de los controles típicos a nivel de transacción que se diseñan con mayor frecuencia para evitar errores financieros. Para los propósitos de esta discusión, todos los esfuerzos, actividades, controles y procesos de mitigación de riesgos instituidos o realizados por la empresa se denominan "controles de mitigación de riesgos de corrupción".

Mapear los controles y otras actividades de mitigación para cada riesgo es importante porque los controles deben ser proporcionales a la probabilidad y los resultados potenciales de la mala conducta. Una vez que se determina el riesgo inherente para cada evento de riesgo de corrupción identificada, la evaluación de riesgos puede proceder con la identificación y catalogación de los controles y procesos de mitigación de riesgos que están en su lugar.

Para muchas empresas grandes, esto suele ser un esfuerzo de múltiples partes interesadas y multifuncional. Si bien algunos controles operan en toda la empresa como parte del entorno de control general, muchos otros están integrados en los procesos comerciales propiedad de funciones individuales, incluidas las ventas, las compras y la logística, o por la gerencia de unidades operativas asociadas con una determinada área geográfica o segmento comercial. Algunos controles pueden ser de naturaleza financiera (por ejemplo, aprobación del informe de gastos de viaje o autorización de pago de facturas del proveedor); otros pueden pertenecer al área legal o de cumplimiento (p. ej.: canales de denuncia de irregularidades), mientras que otros pueden pertenecer a RR.HH. (p. ej.: verificación de antecedentes de los empleados) o líderes empresariales (p.ej.: la identificación y catalogación de los controles, identificación de los factores y evento de riesgo de corrupción).

En el caso de las empresas pequeñas o medianas, la identificación de los controles normalmente se puede centralizar en unos pocos dueños de procesos clave. Para tales empresas, los programas y controles pueden no estar documentados y, como tal, sería importante identificar a las personas y funciones que conocen los controles existentes en esta área. Además, ciertas prácticas, como la separación de funciones y las políticas y procedimientos formales escritos, pueden no existir en dichas empresas debido a limitaciones de recursos. Es aún más importante para tales empresas identificar los controles de mitigación que se encuentran actualmente en práctica o de naturaleza práctica, incluso si no está documentada, como parte de este ejercicio. Como se mencionó anteriormente, para las empresas pequeñas y medianas, un nivel de tolerancia al riesgo establecido sería clave para determinar el costo o beneficio y la necesidad de inversiones adicionales en procedimientos y controles anticorrupción.

Si bien la revisión de la documentación de control y proceso es el paso clave, esto a menudo se complementa con entrevistas y encuestas específicas con las partes interesadas que pueden ayudar a identificar los controles adecuados.

Además, durante este paso, el equipo o la persona que lidera la evaluación de riesgos de corrupción también podría verificar con los dueños de los procesos si los controles y programas de mitigación identificados están realmente funcionando según la política. Esta verificación a veces puede sacar a la luz ciertos procedimientos que pueden ser parte de una política escrita, pero que no se han puesto en práctica.

Al desarrollar una lista de documentos para analizar y una lista de personas para entrevistar, así como preguntas específicas para hacer, puede ser útil comprender una serie de posibles clasificaciones de control. Estos son los más comunes:

1. Controles generales (a nivel de entidad) frente a controles específicos por evento de riesgo (a nivel de proceso).

2. Controles preventivos vs. detectivos.
3. Controles automáticos vs. manuales.

7.4.1 Controles a nivel de entidad frente a controles específicos por evento de riesgo

Al documentar los controles, la empresa debe diferenciar entre controles específicos por evento y controles anticorrupción generales (a nivel de entidad). Es importante identificar los controles a nivel de evento en lugar de solo a nivel de riesgo, ya que diferentes eventos tienden a tener diferentes controles de mitigación.

Hay que tener en cuenta que un evento puede tener varios controles de mitigación, mientras que un solo control puede funcionar con más de un evento. Aunque mantener los controles asignados a los eventos de riesgos de corrupción más probables es un enfoque práctico y de sentido común, la experiencia indica que esto tiende a llevar la evaluación de riesgos por un camino bastante sinuoso. Para evitar no ver el bosque, uno debe tener en cuenta el panorama general y no debe pasar por alto controles más generales que tienen un impacto en la reducción del riesgo. Dichos controles suelen ser de alto nivel y pueden no ser necesariamente específicos de un evento en particular, o incluso pueden no parecer directamente relacionados con el evento, pero su presencia es, no obstante, un factor importante en la reducción general del riesgo.

Por lo tanto, es posible que un proceso de evaluación de riesgos de corrupción que solo considere controles específicos por evento no sea suficientemente sólido y probablemente sea más detallado y requiera más tiempo de preparación que uno que se enfocó primero en los controles a nivel de la entidad y los complementó con el evento -controles específicos donde sea necesario para mitigar el riesgo a un nivel aceptable-. Existe un grado de superposición entre los controles generales y específicos por evento, y algunos controles generales que también aparecen dentro de un cierto evento, generalmente con una variación o especificidad. Es importante tomar nota de los controles que pueden caer en ambas categorías para garantizar que dichos controles se evalúen desde todos los ángulos relevantes. Para obtener una lista de los controles anticorrupción típicos a nivel de entidad, consulte la siguiente Tabla de "Ejemplos de controles anticorrupción".

Ejemplos de controles anticorrupción:

1. Controles anticorrupción generales típicos a nivel de entidad (controles preventivos anticorrupción):
    - Un Sistema de Gestión o Programa de Integridad (contar con un programa formal de lucha contra la corrupción con estructura definida, propiedad, líneas jerárquicas y actividades planificadas, y medición periódica de la eficacia).
    - Un Comité Anticorrupción o de Cumplimiento con el mandato de revisar o recibir actualizaciones sobre todas las transacciones de alto riesgo.
    - Estándares escritos (es decir, el código de conducta, procedimientos anticorrupción y otras políticas para interacción con funcionarios públicos).
    - Capacitación y comunicación anticorrupción para empleados.
    - Comunicación desde arriba y desde el medio: gerencias de alto y medio nivel visibles que establecen las expectativas.
    - Verificación de antecedentes de los empleados.
    - Sistema de canales de denuncia de irregularidades.
    - Aprobación y seguimiento de solicitudes de obsequios, entretenimiento y hospitalidad.
    - Proceso de certificación/divulgación de conflictos de intereses.
    - Disposición sobre cumplimiento en contratos con socios de negocio.
    - Un proceso competitivo de licitación/selección que incluye la difusión de la Política anticorrupción y la revisión de propuestas de los posibles proveedores.
    - Sistema de clasificación de niveles de riesgo para socios de negocio.
    - Debida diligencia a socios de negocios (en línea con el nivel de riesgo designado).
    - Múltiples niveles de aprobación de contratos con socios de negocio o firma compartida (p. ej.: que requieren la aprobación de compras, las funciones legales, de cumplimiento y la gerencia local).

- Controles contables sobre la revisión, aprobación y pago de facturas de socios de negocio.
- Un proceso para la revisión, aprobación y reembolso de informes de gastos y viajes.
- Incorporación de la anticorrupción proactiva en la cultura organizacional.
- Entrevistas de salida.
- Auditorías anticorrupción obligatorias en forma periódica.
- Rotación obligatoria del personal clave de nivel gerencial en ubicaciones de alto riesgo.

Para muchos eventos, los controles preventivos podrían aumentarse mediante controles de detección temprana de faltas de conducta (tanto intencionales como no intencionales).

2. Controles específicos por evento: (Incluidos algunos que pueden ser una versión específica del evento de un control a nivel de entidad.)
   Un evento de riesgo que involucre el uso de socio de negocio/terceras partes puede incluir los siguientes controles y procesos de mitigación:
   - Un proceso para documentar la necesidad de la organización de contratar a un socio de negocio/terceras partes.
   - Debida diligencia/selección de un socio de negocio/terceras partes en aspectos específicos, como verificación de antecedentes, selección de listas de personas políticamente expuestas, verificación de referencias y certificados, compromisos previos, reputación y una muestra de revisión del producto del trabajo (según el nivel de riesgo).
   - Certificación de cumplimiento por parte del socio de negocio/terceras partes (inicial y a intervalos periódicos, por ejemplo, anualmente), como reconocimiento y certificación de su política anticorrupción, el código de conducta, etc.
   - Actividades de capacitación y comunicación anticorrupción dirigidas al personal de compras involucrado, así como a la contratación/gestión continua del socio de negocio/terceras partes.
   - Evaluaciones periódicas del desempeño de los socios de negocio/terceras partes, revisión del producto del trabajo real.
   - Análisis de tarifas/facturas del socio de negocio/terceras partes (¿La factura tiene un nivel adecuado de detalle? ¿Es la tarifa razonable? ¿Cómo se compara con otros proveedores similares? ¿Está acorde con el producto del trabajo? ¿Existe una correlación entre una factura del socio de negocio/terceras partes y una acción de gobierno que benefició a la empresa?, etc.).

   Un evento que involucra a representantes de ventas de empresas comerciales que brindan obsequios, hospitalidad y entretenimiento potencialmente inapropiados a prospectos o clientes puede incluir lo siguiente:
   - Capacitación y comunicación periódicas sobre obsequios y entretenimiento dirigidas al personal de ventas y sus gerentes.
   - Comunicación a los clientes sobre la política de obsequios, hospitalidad y entretenimiento de la empresa.
   - Comunicación de los supervisores o liderazgo con el personal de ventas.
   - Reconocimiento o certificación periódica (por ejemplo, anual) de la política anticorrupción entre el personal de ventas y los supervisores.
   - Uso obligatorio de las tarjetas de crédito de la empresa para comidas con terceros u otro entretenimiento del personal de ventas.
   - Rotación de representantes de ventas.
   - Encuesta/entrevistas a clientes.
   - Disponibilidad de línea directa para el personal del cliente.

3. Controles de detección anticorrupción:
   - Seguimiento de obsequios, hospitalidad y entretenimiento (después del hecho).

- Auditoría del informe de gastos.
- Monitoreo periódico de terceros (por ejemplo: evaluación del desempeño, recertificación).
- Proceso de alerta temprana efectivo sobre indicadores de riesgo de soborno e identificación y comunicación de *Red Flags*.
- Sistema de canales de denuncia de irregularidades, proceso de investigación y gestión de casos.
- Identificación y análisis sistemático de vulnerabilidades y su monitoreo.
- Entrevistas de salida.
- Auditoría corporativa, auditoría de transacciones, auditoría de terceros.
- La cultura de la ética de los empleados y la evaluación del cumplimiento, particularmente, si incluye preguntas sobre la presión para cometer una mala conducta, violaciones reales de políticas, etc.
- Encuesta o entrevista a clientes, proveedores o terceros.

Los controles específicos de evento pueden, naturalmente, variar según el evento específico y otros factores, como la geografía de operación, la naturaleza de los productos y/o servicios, los tipos de clientes y el modelo comercial en cuestión, la composición de la fuerza laboral y la naturaleza de otros terceros.

7.4.2 Controles preventivos frente a controles detectivos

Al catalogar los controles de mitigación de riesgos, puede ser útil tener en cuenta el propósito de dichos controles. No toda mala conducta es intencionada. Algunas pueden ser el resultado de negligencia o falta de concientización. En tales situaciones, los controles preventivos, como políticas claras, capacitación y comunicación, juegan un papel clave en la mitigación efectiva. Por otro lado, la mala conducta intencional está pensada, organizada y orquestada para evadir la detección. Los controles preventivos son importantes y generalmente efectivos para prevenir algunos actos potenciales de corrupción, particularmente aquellos que son de escala relativamente pequeña o resultan de una falta de concientización, como los que caen en el área gris de la hospitalidad excesiva sin una intención corrupta. Sin embargo, los controles preventivos pueden no ser suficientes para desanimar o disuadir a un posible perpetrador intencional y, como sugiere el nombre, generalmente no están diseñados para funcionar como controles detectivos.

Si bien la experiencia muestra que la presencia de un sólido cuerpo de controles preventivos, incluida una sólida cultura ética y un entorno de cumplimiento en la empresa, es probable que desaliente un poco a los perpetradores intencionales de intentarlo, incluso las empresas más éticas tienen el caso ocasional de una "manzana podrida" que intentará evadir el sistema.

Aquí es donde entran en juego los controles detectivos. El propósito de los controles detectivos es ayudar a detectar las irregularidades, idealmente, en una etapa temprana.

Es deseable que los controles y procedimientos detectivos incluyan algunos de los que el perpetrador puede no estar al tanto o no esperar razonablemente.

Para tener un buen sistema de detección de corrupción, la identificación de tales controles requiere un grado de "razonamiento estratégico" para anticipar el comportamiento de un perpetrador potencial. El razonamiento estratégico requiere una mentalidad escéptica e implica hacer preguntas como:

- ¿Cómo podría un perpetrador explotar las debilidades en el sistema de controles?
- ¿Cómo podría un perpetrador anular o eludir los controles?
- ¿Qué podría hacer un perpetrador para ocultar… [un acto corrupto]?

La mayoría de los controles identificados pueden etiquetarse como preventivos o detectivos, aunque algunos pueden tener un doble propósito. Catalogar los controles ayudará a calibrar la estrategia de mitigación de riesgos y el plan de respuesta de acuerdo con la naturaleza de la mala conducta de corrupción real o potencial esperada.

7.4.3 Marcos del mapeo de control anticorrupción

Los profesionales de la evaluación de riesgos de corrupción tienen una amplia variedad de marcos que pueden usarse para catalogar y clasificar controles y otros esfuerzos de mitigación de riesgos. Los siguientes seis son los más utilizados:

1. Los doce elementos de un programa efectivo de cumplimiento anticorrupción de la Guía de buenas prácticas de la OCDE sobre controles internos, ética y cumplimiento.
2. Los seis principios de la Orientación del Ministerio de Justicia del Reino Unido sobre la Ley de sobornos de 2010.
3. Los siete "sellos distintivos para un programa de cumplimiento efectivo", promulgados por las Pautas Federales de Sentencia (*FSG*) de EE. UU.
4. Trece pasos en un programa de cumplimiento corporativo para la *FCPA*, según lo establecido por el Departamento de Justicia de EE. UU. con respecto a múltiples acuerdos de enjuiciamiento diferido y acuerdos de no enjuiciamiento.
5. Los Principios Comerciales para Contrarrestar el Soborno emitidos por Transparencia Internacional.
6. Programa de cumplimiento y ética anticorrupción para empresas de la *UNODC*: una guía práctica.
7. Los lineamientos de integridad emitidos por la Oficina Anticorrupción (OA) para el mejor cumplimiento de lo establecido en los artículos 22 y 23 de la Ley N° 27.401 de Responsabilidad Penal de las Personas Jurídicas (2.2. Carácter adecuado del Programa y 2.5. Evaluación inicial de riesgos).

Al identificar sus procesos y controles de mitigación de riesgos de corrupción, puede ser útil comenzar con controles generales y luego limitarse a eventos de riesgos específicos, utilizando el marco de los sellos distintivos de la *FSG* de EE. UU.

El inventario de controles generales (controles a nivel de entidad o "familias" de control) incluye:

1. Estructura y recursos del programa: un programa formal de cumplimiento anticorrupción, con estructura, propiedad, autoridad, plan de actividades y presupuesto definidos.
2. Supervisión del programa: informes de las relaciones y supervisión del programa por parte de las autoridades internas pertinentes.
3. Normas escritas: un código de conducta y políticas relevantes.
4. Procesos de diligencia debida: verificación de antecedentes de los empleados y diligencia debida inicial de terceras partes, separación de funciones, límites de autoridad, revisión y aprobación de contratos (proveedores, clientes) y disposiciones de cumplimiento en contratos de terceros.
5. Capacitación y comunicación: programas formales de capacitación, comunicación periódica a los empleados, disponibilidad de orientación y recursos para el empleador y compromiso visible de los gerentes *(Tone from the top and the middle*).
6. Monitoreo y auditoría: un sistema de canal de denuncia de irregularidades, con un fuerte enfoque en no represalias, seguimiento de obsequios y entretenimiento, proceso de aprobación y reembolso de gastos, sistema de niveles de riesgo, sistemas de auditoría y monitoreo continuo de terceras partes/socios de negocio, auditoría de transacciones y gastos corporativos, evaluaciones de desempeño de empleados y proveedores, entrevistas de salida de empleados, evaluación de la cultura de ética y cumplimiento y evaluación periódica del programa anticorrupción.
7. Ejecución: investigación de mala conducta y proceso de gestión de casos, proceso disciplinario y comunicación, e incentivos de ética y cumplimiento.

Si bien los controles a nivel de entidad son más adecuados para la clasificación de acuerdo con uno de los marcos anteriores, la mayoría de los controles específicos por evento de riesgo también se pueden etiquetar en consecuencia.

7.4.4 Incluir controles de mitigación en el registro de riesgos

Ubicación/Región			
Unidad de Negocio: Unidad XYZ			
Categoría de riesgo de corrupción	**Riesgo estratégico**	**Riesgos de Integridad**	**Riesgos relacionados con Socios de Negocio**
Evento del riesgo de corrupción	No proporcionar un alto nivel de integridad, transparencia y fiabilidad del servicio y la entrega de productos y garantizar una mejora continua.	No impedir el soborno a un funcionario con el objetivo de facilitar la expedición de licencias, permisos, certificados y otros tipos de servicios públicos.	Fallar en asegurar la participación de los socios de negocio en la política de tolerancia cero al soborno y la corrupción de la entidad.
Consecuencias de la falla	Financieros, legales, regulatorios, operativos y de reputación.	Financieros, legales, regulatorios, operativos y de reputación.	Daño del patrimonio institucional, daño de la imagen y reputación.
Causa de la falla	Fallar en el compromiso estratégico del liderazgo	Fallar en la toma de conciencia y formación.	Falta de difusión de la cultura corporativa.
Probabilidad	2	3	1
Impacto potencial	4	5	3
Riesgo inherente	**8 Importante**	**15 Inaceptable**	**3 Aceptable**
Control anticorrupción	Prueba de controles internos antisoborno	Hallazgos de las auditorías internas y externas.	Política robusta del canal de denuncias y alerta temprana.

Una vez que todos los controles existentes han sido identificados, categorizados y etiquetados apropiadamente y referenciados, el proceso de evaluación de riesgos está listo para continuar con su siguiente paso: calificación del control.

7.5 Calificación de controles y procesos de mitigación (EB)

La calificación de los controles de mitigación de riesgos de una empresa puede ser fundamental para determinar los riesgos residuales. Antes de que pueda comenzar la calificación de control, las empresas deben pensar en la profundidad deseada del ejercicio, los criterios utilizados, la escala de calificación y

los mecanismos de recopilación de datos disponibles (por ejemplo: encuestas, entrevistas, evaluación de documentos, etc.).

Hay muchas formas diferentes de calificar la efectividad de los controles de mitigación. Se podría utilizar una escala cuantitativa con puntuaciones aplicadas con criterio a cada evento de riesgo. La siguiente tabla "Matriz de puntaje para la clasificación de control" incluye un ejemplo de cómo pueden verse los criterios de calificación.

7.5.1 Matriz de puntaje para la clasificación de control

Muestra de matriz de puntaje de escala de 5 puntos para el puntaje de control		
Categorización cualitativa	**Categorización numérica**	**Calificación de efectividad del control**
Excelente y muy efectiva	1	Muy alto
Buena y efectiva	2	Alto
Justa/neutral/parcialmente efectiva	3	Medio
Pobre / Algo efectiva	4	Bajo
Muy pobre / ineficaz	5	Muy bajo

El resultado final de la evaluación del control suele ser una tarjeta de puntuación, en la que cada control se muestra con una puntuación de "calidad" cualitativa o numérica y un comentario subyacente.

Los criterios de evaluación de los controles pueden variar mucho según los controles en cuestión, el nivel de profundidad deseado para la evaluación y la experiencia del personal de evaluación de riesgos de corrupción. Si bien algunos controles pueden tener solo unos pocos criterios utilizados como base para la calificación, no es inusual tener hasta varias docenas de criterios de evaluación distintos por control principal en una evaluación sofisticada y profunda. Las evaluaciones de nivel superior bien pueden reducir el nivel de detalle.

Cualquier tipo de puntuación invita a cuestionar la precisión y la objetividad. Los criterios detallados y basados en hechos (en lugar de simplemente en la percepción) aumentan ambos. El uso de múltiples tipos de fuentes de información en el proceso de calificación también ayuda a lograr una mayor precisión y objetividad, así como a validar algunos de los datos y puntajes, particularmente aquellos con un sesgo subjetivo. Si bien la calificación de riesgo de control generalmente se basa en el juicio de las personas involucradas en la calificación, para las empresas que han realizado pruebas o auditorías independientes de controles anticorrupción, los resultados tendrían una gran influencia en la calificación de riesgo de control asignada (por ejemplo: si los resultados de la prueba revelan que un control está funcionando eficazmente, normalmente se le daría una calificación de "eficaz" o "riesgo de control bajo").

Un enfoque para realizar la calificación es que los dueños de procesos asignen juiciosamente una puntuación basada en consideraciones cualitativas (y este es un enfoque que utilizarían la mayoría de las pequeñas o medianas empresas). Sin embargo, se podría emplear un enfoque más integral para determinar las calificaciones de riesgo de control con el fin de adoptar más estructura, objetividad y precisión en el proceso. A continuación, se enumeran ejemplos de fuentes y mecanismos de recopilación de datos relacionados para el enfoque más integral.

7.5.2 Revisión y evaluación de documentos internos

Un gran punto de partida y fuente de datos para muchas preguntas relacionadas con la calificación de controles pueden incluir:

- Formularios y documentación de procesos (por ejemplo: formulario de informe de gastos y proceso de aprobación, proceso de diligencia debida de terceras partes/socios de negocios y formularios relacionados).
- Procedimientos estandarizados.

- Organigramas.
- Modelos y muestras de contratos.
- Documentación de herramientas de seguimiento de obsequios y entretenimiento.
- Resultados de encuestas de empleados anteriores.
- Estadísticas de denuncia de irregularidades y expedientes de investigación de conducta indebida.
- Notas de la entrevista de salida.
- Informes de auditoría interna y externa.

7.5.3 Entrevistas en vivo

Las entrevistas en vivo, que a menudo se utilizan para complementar y validar los datos recibidos a través de la revisión de la documentación, pueden ser un método eficaz para obtener información cualitativa adicional y más detallada cuando los documentos pueden no proporcionar una imagen completa. Cuando una empresa carece de documentación, o tiene dificultades para obtener información, el valor de las entrevistas aumentará exponencialmente. La audiencia de la entrevista está formada generalmente por los dueños de procesos de negocio clave con conocimiento del proceso y controles para el área aplicable. Estas entrevistas pueden combinarse con las entrevistas para identificar los riesgos en el paso 2 del proceso o pueden realizarse por separado.

7.5.4 Encuestas sobre "Entorno de cumplimiento y control"

Si el número de personas enumeradas para las entrevistas en vivo es demasiado grande para manejarlo y/o incluye un número de individuos homogéneos (p.ej.: funciones o roles idénticos en diferentes regiones), lo que permite cierto grado de uniformidad para muchas preguntas, las encuestas en línea específicas pueden ser una alternativa eficaz al menos para algunas entrevistas en vivo y un buen complemento a una encuesta masiva de empleados ("evaluación de la cultura y el conocimiento") y la evaluación de documentos.

Este tipo de encuesta suele ser una "evaluación del entorno de cumplimiento y control" que se da a las partes interesadas clave en el programa anticorrupción, la Alta Dirección y terceras partes/socios de negocio. Estas encuestas están bastante personalizadas para el público objetivo en cuestión y, por lo general, incluyen una combinación de preguntas de opción múltiple y preguntas abiertas. La encuesta generalmente solicita la opinión del encuestado sobre controles, procesos e iniciativas de mitigación de riesgos particulares, y puede ser anónima o no.

Mientras que una encuesta masiva de empleados (ya sea una evaluación de la cultura y el conocimiento o una encuesta dedicada a los empleados sobre corrupción) para una gran empresa puede llegar fácilmente a miles o incluso a decenas de miles de encuestados, las encuestas de "entorno de control y cumplimiento" rara vez superan varios cientos de personas, incluso para una gran empresa, y a menudo están dirigidas a menos de cien encuestados, generalmente, en un nivel bastante alto o en puestos clave.

7.5.5 Grupos focales y talleres

Los grupos focales y los talleres pueden ser una herramienta eficaz para realizar un examen exhaustivo de un tema en particular o un problema para un control o proceso. A menudo, este método de recopilación de datos se lleva a cabo *in situ* con una pequeña audiencia de 5 a 10 personas, ya sea de una sola función (por ejemplo, ventas) o interfuncionalmente en un mercado dado (por ejemplo, una región). Otras versiones son de función única (generalmente de nivel superior) a nivel mundial; por ejemplo, en una conferencia interna de cumplimiento global o una reunión de ventas global. Estos grupos focales y talleres podrían combinarse con aquellos encargados de realizar la identificación de riesgos y/o calificaciones de riesgo heredadas.

7.5.6 ¿Quién debe participar en los cálculos de calificación de riesgo de control?

Es importante involucrar solo a aquellas personas que están familiarizadas con el control o proceso que se está calificando, incluidos los dueños del proceso.

Se podría buscar las opiniones de más de un individuo para ciertos controles, en cuyo caso se podría tomar un promedio de la puntuación.

Una de las funciones del dueño de una evaluación de riesgos de corrupción podría ser evaluar si las puntuaciones brutas designadas por las partes relevantes son razonables y hacer sugerencias para cuestionar o reevaluar cualquier calificación que parezca cuestionable.

Al igual que en el cálculo del riesgo inherente, los protocolos para estimar y cuestionar las calificaciones deben determinarse por adelantado, debido a las mismas preocupaciones por llegar a un resultado que represente con precisión a la empresa.

7.5.7 Inclusión de la calificación de riesgo de control en el Registro de riesgo

Las calificaciones generales de riesgo de control asignadas para cada evento de riesgo pueden incluirse en el Registro de riesgos de la siguiente manera:

Ubicación/Región			
Unidad de Negocio: Unidad XYZ			
Categoría de riesgo de corrupción	**Riesgo estratégico**	**Riesgos de Integridad**	**Riesgos relacionados con Socios de Negocio**
Evento del riesgo de corrupción	No proporcionar un alto nivel de integridad, transparencia y fiabilidad del servicio y la entrega de productos y garantizar una mejora continua.	No impedir el soborno a un funcionario con el objetivo de facilitar la expedición de licencias, permisos, certificados y otros tipos de servicios públicos.	Fallar en asegurar la participación de los socios de negocio en la política de tolerancia cero al soborno y la corrupción de la entidad.
Consecuencias de la falla	Financieras, legales, regulatorias, operativas y de reputación.	Financieras, legales, regulatorias, operativas y de reputación.	Daño del patrimonio institucional, daño de la imagen y reputación.
Causa de la falla	Fallar en el compromiso estratégico del liderazgo.	Fallar en la toma de conciencia y formación.	Falta de difusión de la cultura corporativa.
Probabilidad	2	3	1
Impacto potencial	4	5	3
Riesgo inherente	**8 Importante**	**15 Inaceptable**	**3 Aceptable**
Control anticorrupción	Prueba de controles internos antisoborno	Hallazgos de las auditorías internas y externas	Política robusta del canal de denuncias y alerta temprana
Clasificación de control anticorrupción	**2 Buena y efectiva**	**5 Muy pobre / ineficaz**	**3 Justa/neutral/parcialmente efectiva**

7.6 Cálculo del riesgo residual (EB)

Después de calificar los controles internos que reducen el riesgo de cada evento de riesgo, el siguiente paso es determinar el nivel de riesgo residual.

El riesgo residual es el alcance del riesgo que queda después de considerar el impacto de los controles en la reducción del riesgo. El riesgo residual es un factor del riesgo inherente y el riesgo de control.

A pesar de los programas anticorrupción y sus controles internos para mitigar el riesgo de que ocurran fallas en los eventos de riesgos de corrupción, por lo general todavía es posible que ocurran. Como resultado, normalmente habrá algún nivel de riesgo residual para cada evento de riesgo. Un riesgo residual de cero es teóricamente posible para un evento de riesgo de corrupción en particular, pero esto normalmente surgiría solo si ese evento de riesgo no fuera relevante para las operaciones de la empresa, por ejemplo, porque no realizó negocios en una industria en particular o de una manera particular. La medida en que los controles internos mitigan el riesgo de un evento de riesgo de corrupción depende de qué tan bien se diseñen, implementen y operen los controles para reducir efectivamente el riesgo de ese evento en particular.

Los controles que están bien diseñados para mitigar los riesgos que surgen de uno o varios eventos de riesgos de corrupción, que se han implementado apropiadamente y que están operando efectivamente en la práctica, pueden reducir, en gran medida, el riesgo que surge de un evento en particular.

7.6.1 Escala cualitativa para determinar el riesgo residual

Si el riesgo inherente es:	Y la calificación de riesgo de control es:	Entonces el riesgo residual es normalmente:
Inaceptable	**Bajo**	**Alto**
Inaceptable	**Medio**	**Alto**
Inaceptable	**Alto**	**Medio**
Importante	**Bajo**	**Alto**
Importante	**Medio**	**Medio**
Importante	**Alto**	**Bajo**
Moderado	**Bajo**	**Medio**
Moderado	**Medio**	**Medio**
Moderado	**Alto**	**Bajo**
Aceptable	**Bajo**	**Bajo**
Aceptable	**Medio**	**Bajo**
Aceptable	**Alto**	**Bajo**

Las calificaciones de riesgo residual proporcionarán a la gerencia una evaluación de dónde puede existir su mayor exposición a riesgos de corrupción. Una calificación de riesgo residual alta significaría que los controles no mitigan sustancialmente un riesgo de corrupción inherente de alta calificación, lo que deja un riesgo residual que podría afectar seriamente a la empresa. Un riesgo residual medio significaría que el evento de riesgo de corrupción es inherentemente de alto riesgo y parcialmente mitigado por

los controles o un riesgo inherentemente mediano y no se mitiga sustancialmente o en absoluto con los controles. Un riesgo residual bajo significaría que el evento de riesgo de corrupción es inherentemente un riesgo de baja calificación o que está sustancialmente mitigado por controles.

Debido a problemas de recursos o costos, algunas empresas pueden optar por no incluir el cálculo del riesgo residual de manera explícita en su proceso de evaluación del riesgo de corrupción. Si bien no es el enfoque óptimo, se podría realizar una evaluación del riesgo anticorrupción con solo una determinación del riesgo inherente junto con la identificación de los controles de mitigación. Sin embargo, dado que la gerencia aún tendría que considerar si creía que sus riesgos de corrupción se habían mitigado adecuadamente, es posible que aún estén haciendo juicios implícitos sobre el nivel de riesgo residual. Una evaluación explícita del riesgo residual es más transparente y proporciona una herramienta de trabajo que facilita enormemente la discusión abierta y sincera entre la gerencia y otras partes interesadas, como los encargados de la gobernanza, con respecto a la exposición de la empresa a los riesgos de corrupción.

7.6.2 Inclusión del riesgo residual en el registro de riesgos

El riesgo residual total asignado para cada riesgo o evento de riesgo puede incluirse en el registro de riesgos de la siguiente manera:

Ubicación/Región			
Unidad de Negocio: Unidad XYZ			
Categoría de riesgo de corrupción	**Riesgo estratégico**	**Riesgos de Integridad**	**Riesgos relacionados con Socios de Negocio**
Evento del riesgo de corrupción	No proporcionar un alto nivel de integridad, transparencia y fiabilidad del servicio y la entrega de productos y garantizar una mejora continua.	No impedir el soborno a un funcionario con el objetivo de facilitar la expedición de licencias, permisos, certificados y otros tipos de servicios públicos.	Fallar en asegurar la participación de los socios de negocio a la política de tolerancia cero al soborno y la corrupción de la entidad.
Consecuencias de la falla	Financieros, legales, regulatorios, operativos y de reputación.	Financieros, legales, regulatorios, operativos y de reputación.	Daño del patrimonio institucional, daño de la imagen y reputación.
Causa de la falla	Fallar en el compromiso estratégico del liderazgo.	Fallar en la toma de conciencia y formación.	Falta de difusión de la cultura corporativa.
Probabilidad	2	3	1
Impacto potencial	4	5	3
Riesgo inherente	**8 Importante**	**15 Inaceptable**	**3 Aceptable**
Control anticorrupción	Prueba de controles internos antisoborno.	Hallazgos de las auditorías internas y externas.	Política robusta del canal de denuncias y alerta temprana.
Clasificación de control anticorrupción	**2 Buena y efectiva**	**5 Muy pobre / ineficaz**	**3 Justa/neutral/ parcialmente efectiva**
Calificación de riesgo residual	**BAJO**	**ALTO**	**BAJO**

7.7 Planes de respuesta al riesgo de corrupción (EB)

7.7.1 Comparación del riesgo residual con la tolerancia al riesgo

Una empresa puede evaluar el riesgo residual de cada evento de riesgo para determinar si se necesita una respuesta al riesgo de corrupción y, de ser así, los elementos deseados de ese plan. Un determinante clave del plan de respuesta es el nivel de tolerancia al riesgo o el apetito por el riesgo de la empresa, que variará según la empresa.

No se requiere más mitigación del riesgo para cualquier evento de riesgo de corrupción que tenga un riesgo residual dentro de la tolerancia al riesgo establecida por la gerencia y aprobada por los encargados del gobierno corporativo. La gerencia puede optar por implementar una mitigación de riesgos adicional si cree que el costo-beneficio puede ser una ventaja, pero no es esencial.

Para cualquier evento de riesgo que tenga un riesgo residual mayor que la tolerancia al riesgo establecida por la gerencia y aprobada por los encargados del gobierno corporativo, es necesario tomar medidas para reducir el riesgo hasta que esté dentro del umbral de tolerancia al riesgo. Para estos elementos, se necesita un plan de respuesta al riesgo de corrupción.

7.7.2 Respuestas potenciales a los riesgos residuales que superan la tolerancia al riesgo

Históricamente, la respuesta más común a los riesgos residuales de corrupción fue implementar mejoras en los controles internos para aumentar la mitigación del riesgo de corrupción. Las empresas líderes consideran una gama más amplia de posibles acciones para abordar el riesgo de corrupción residual, que incluyen:

- Cambiar el alcance del negocio de la empresa, como evitar o detener la realización de negocios en ciertas geografías, segmentos de la industria o mercados porque se considera que el riesgo es imposible de mitigar de manera suficiente y confiable.
- Cambiar los procesos o métodos comerciales para reducir o eliminar el área de riesgo, como cambiar de vender bienes “CIF” (costo, seguro y flete) a Ex Works, lo que significa que el comprador se haría cargo de los bienes en el lugar de trabajo del vendedor y sería responsable de los costos de transporte y del despacho de aduana para envíos internacionales. Este arreglo puede eliminar los riesgos del vendedor relacionados con el posible soborno de funcionarios gubernamentales extranjeros para obtener el despacho de aduana en el puerto de destino.
- Transferir riesgos a un tercero a través de términos contractuales.
- Mejora de ciertos controles anticorrupción.

7.7.3 Plan de respuesta al riesgo de corrupción

Cabe señalar que no todas las empresas tienen los mismos recursos y fondos a su disposición para invertir al mismo nivel en el programa de cumplimiento anticorrupción.

Es posible que algunas empresas solo deseen abordar programas y controles para lo que consideran las áreas de exposición más importantes, mientras que otras pueden querer abordar más el interés de mantener un programa de cumplimiento anticorrupción más sólido. Si bien la necesidad de una respuesta debe evaluarse en función de la tolerancia al riesgo de la empresa y las limitaciones de recursos, las cuales variarán de una empresa a otra, a menudo se observan algunos enfoques:

- Los eventos de riesgos de corrupción que tienen un riesgo residual de “alto” generalmente exceden la tolerancia de la empresa al riesgo residual y es probable que se les preste atención, ya que esta calificación indica un nivel de riesgo que puede representar una amenaza grave o potencialmente catastrófica a la empresa.

- Los eventos de riesgos que tienen un riesgo residual de "medio" pueden o no exceder la tolerancia de la empresa al riesgo residual, por lo que la acción puede ser necesaria o no. La gerencia podría analizar la calificación de riesgo inherente y la calificación de riesgo de control para evaluar las fuentes de riesgo y considerar la viabilidad de una mitigación de riesgo adicional para determinar si tomar más medidas.
- Para los eventos de riesgos de corrupción que tienen un riesgo residual de "bajo", una empresa normalmente no tomaría más medidas.

Algunas empresas pueden optar por tener una respuesta para las áreas de riesgo residual "alto" y decidir no tomar ninguna acción para las áreas de riesgo residual "medio" o "bajo" como parte de la estrategia de tolerancia al riesgo. Otros pueden priorizar las acciones, con aquellas que abordan áreas de riesgo residual "alto" como la prioridad más alta, seguidas de áreas de riesgo residual "medio" y "bajo".

En tales casos, se puede tomar acciones en función del tiempo y los recursos disponibles, así como del juicio de la gerencia.

Para las pequeñas y medianas empresas, el plan de respuesta al riesgo de corrupción es una herramienta importante para determinar si se necesita alguna inversión de recursos para mitigar los riesgos de corrupción y, de ser así, a qué áreas asignar los recursos. Estas empresas pueden usar este plan de respuesta para determinar cuál de los diversos elementos del programa anticorrupción (por ejemplo, políticas específicas, capacitación, monitoreo, etc.) necesitan implementar o mejorar en función de los riesgos. Las empresas pequeñas y medianas generalmente no tienen suficiente exposición al riesgo para garantizar políticas y controles sólidos en cada elemento del programa anticorrupción y los resultados de la evaluación del riesgo anticorrupción pueden ser una herramienta valiosa para que dichas empresas determinen cuál de cualquiera de estos elementos que quieran implementar o mejorar.

Revisión continua: el control es adecuado, continuar el seguimiento de los controles para confirmarlo, es decir, al menos trimestralmente.
Gestión activa: riesgos donde las opciones de tratamiento actuales requieren preparación, revisión activa y manejo de manera continua.
Sin mayor preocupación: riesgos donde los sistemas y procesos que gestionan el riesgo son adecuados. Considere controles excesivos o redundantes.
Revisión periódica: el control no es fuerte pero la consecuencia del riesgo no es alta. Las opciones son mejorar el control o monitorear la consecuencia del riesgo para garantizar que no aumente con el tiempo.

Se ilustra un ejemplo de un enfoque para determinar el plan de respuesta al riesgo de corrupción.

7.7.4 Contenido del plan de respuesta

Los comentarios sobre los elementos propuestos para su inclusión en el plan de respuesta al riesgo de corrupción deben provenir de toda la organización, incluidas las opiniones de esas funciones y las personas responsables de implementar los elementos de acción y aquellos afectados por los posibles elementos de acción. Es importante que el plan de respuesta al riesgo de corrupción sea pragmático y

selectivo, ya que existe un sinfín de controles internos que podrían implementarse en cada empresa. Un buen plan de respuesta al riesgo de corrupción será selectivo y específico, basado en un enfoque práctico y estructurado que reduce de manera eficiente y efectiva los riesgos residuales dentro de la tolerancia al riesgo de la empresa. Una vez que se redacta un plan de respuesta al riesgo, generalmente es aprobado por la gerencia responsable de la evaluación del riesgo de corrupción, con la supervisión de los encargados del gobierno corporativo.

Algunas de las características de un plan de respuesta pueden incluir:

- Descripción de cada elemento de acción.
- Responsable de implementación para cada elemento de acción.
- Calendario de implementación. Si bien cada elemento generalmente se aborda dentro de un período de doce meses (y algunos con bastante rapidez), podría haber situaciones en las que una empresa opte por implementar ciertos elementos del plan de respuesta al riesgo de corrupción en el primer año y el resto se completará posteriormente en una escala de priorización. Para plazos de mediano a largo plazo, se puede incluir hitos seleccionados en el plan de respuesta al riesgo de corrupción.
- Estimación de los recursos necesarios para abordar cada elemento de acción, como el número de personas, las horas y el presupuesto.

Es deseable que una persona sea responsable de coordinar la implementación del plan de respuesta al riesgo de corrupción y de informar a la administración y, posiblemente, a los encargados del gobierno corporativo. La implementación debe ser monitoreada regularmente por la gerencia con cualquier enmienda necesaria o apropiada hecha por la gerencia y aprobada por los encargados del gobierno corporativo.

Ubicación/Región			
Unidad de Negocio: Unidad XYZ			
Categoría de riesgo de corrupción	**Riesgo estratégico**	**Riesgos de Integridad**	**Riesgos relacionados con Socios de Negocio**
Evento del riesgo de corrupción	No proporcionar un alto nivel de integridad, transparencia y fiabilidad del servicio y la entrega de productos y garantizar una mejora continua.	No impedir el soborno a un funcionario con el objetivo de facilitar la expedición de licencias, permisos, certificados y otros tipos de servicios públicos.	Fallar en asegurar la participación de los socios de negocio para la política de tolerancia cero al soborno y la corrupción de la entidad.
Consecuencias de la falla	Financieros, legales, regulatorios, operativos y de reputación.	Financieros, legales, regulatorios, operativos y de reputación.	Daño del patrimonio institucional, daño de la imagen y reputación.
Causa de la falla	Fallar en el compromiso estratégico del liderazgo.	Fallar en la toma de conciencia y formación.	Falta de difusión de la cultura corporativa.
Probabilidad	2	3	1
Impacto potencial	4	5	3
Riesgo inherente	**8 Importante**	**15 Inaceptable**	**3 Aceptable**
Control anticorrupción	Prueba de controles internos antisoborno.	Hallazgos de las auditorías internas y externas.	Política robusta del canal de denuncias y alerta temprana.
Clasificación de control anticorrupción	**2 Buena y efectiva**	**5 Muy pobre / ineficaz**	**3 Justa/neutral/parcialmente efectiva**
Calificación de riesgo residual	**BAJO**	**ALTO**	**BAJO**
Plan de respuesta:			
Dueño del riesgo	N/A	Oficial de cumplimiento y todas las áreas del proceso sujeto a alcance.	Oficial de cumplimiento
Fecha objetivo	N/A	16 de mayo 2024	Permanente
Acciones Recomendadas	N/A	Toma de conciencia y formación.	Debida diligencia con determinadas categorías de socios de negocios.

7.7.5 Participación del liderazgo

Un tema crítico para la implementación exitosa del plan de respuesta al riesgo de corrupción suele ser la aceptación del Órgano de gobierno, la Alta Dirección, el comité de auditoría u otros encargados del gobierno corporativo. Sin ese apoyo de alto nivel, la implementación del plan de respuesta puede estancarse, ya que ciertas funciones o personas pueden no brindar la importancia y atención necesarias a los elementos del plan de respuesta.

Además, sería beneficioso para el dueño de la evaluación de riesgo de corrupción explicar a los diversos actores involucrados por qué la implementación de los pasos en el plan de respuesta puede beneficiarlos tanto individualmente como en grupo. Una estrategia consiste en vincular el progreso en la finalización de los elementos del plan de respuesta con los objetivos de las personas y las funciones y la evaluación del desempeño. Otra estrategia consiste en involucrar a las distintas partes interesadas en las primeras etapas del proceso de evaluación del riesgo de corrupción y no esperar hasta que sea necesario implementar el plan de respuesta.

7.8 Resumen y presentación de informes de los resultados de una evaluación de riesgos de corrupción (EB)

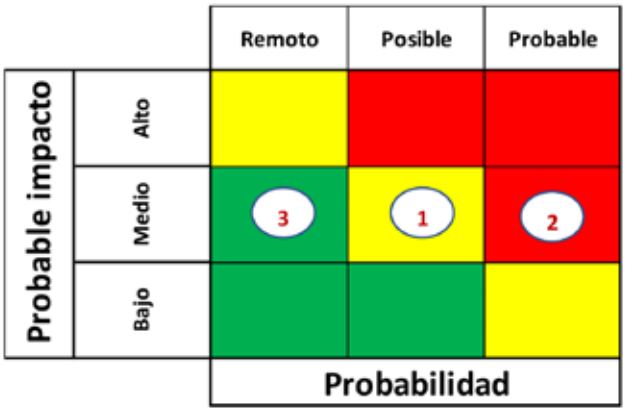
7.8.1 Mapas de calor

Las evaluaciones de riesgos de corrupción a menudo se documentan mediante hojas de cálculo detalladas, como el Registro de riesgos. Estos son convenientes para registrar información relacionada con muchos riesgos, pero su salida puede ser voluminosa, muy detallada y en letra pequeña. Todos estos factores pueden hacer que dichos informes sean ineficaces para comunicar los resultados resumidos a la gerencia y los encargados del gobierno corporativo. Se necesita una forma más sencilla de resumir la información más importante en una hoja de papel y comunicarla de una manera que se entienda rápida y fácilmente.

Los mapas de calor pueden resumir de manera eficaz los resultados de la evaluación de riesgos de corrupción y presentarlos de manera impactante a la gerencia y a los encargados del gobierno corporativo. Un mapa de calor de riesgo de corrupción muestra los riesgos identificados por la empresa, colocados de acuerdo con su probabilidad e impacto potencial, sobre un fondo de varios colores, que representan diferentes niveles generales de riesgo. Los mapas de calor simples suelen tener secciones en rojo, amarillo o verde, que indican alto riesgo, riesgo medio y riesgo bajo, respectivamente. Los mapas de calor más complejos utilizan varios tonos de cada color para mostrar variaciones sutiles de la puntuación de riesgo general. Estos pueden representar mejor las variaciones en los puntajes de riesgo individuales, pero los mapas de calor más simples pueden ser más rápidos y fáciles de comprender para los ejecutivos. Esto puede permitir que los ejecutivos dediquen menos tiempo a comprender los datos y más tiempo a analizar detenidamente los problemas clave de riesgo.

Los mapas de calor se pueden utilizar tanto para ilustrar una vista consolidada de toda la empresa como para ilustrar las vistas por ubicación, unidad de negocio o función.

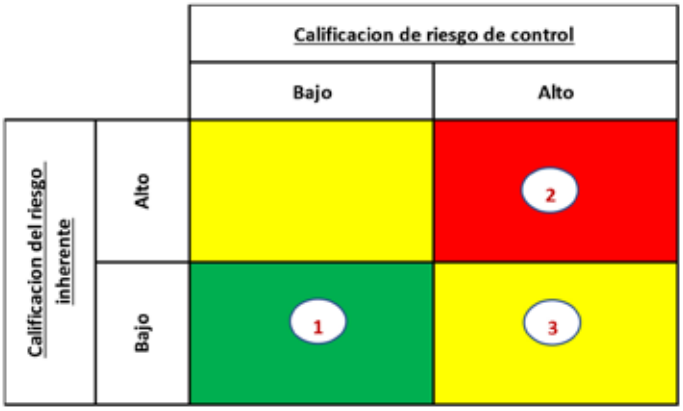
Se muestra un ejemplo de un fondo de mapa de calor simple antes de que se agreguen los riesgos de corrupción individuales. Para compilar un mapa de calor simple a partir de un mayor volumen de datos, una empresa puede agrupar los eventos de riesgos de corrupción particulares para establecer una calificación o puntuación de categoría amplia tanto para el riesgo inherente como para el riesgo de control. Por ejemplo, un área de riesgo de corrupción puede tener varios eventos de riesgos asociados, y cada evento de riesgo puede tener diferentes puntajes cuantitativos de riesgo inherente y riesgo de control. Para llegar a una puntuación cuantitativa para cada riesgo inherente y riesgo de control, una empresa puede tomar el promedio de las puntuaciones de riesgo inherente y de riesgo residual de todos los eventos de riesgos. Alternativamente, para una escala cualitativa, una empresa puede asignar juiciosamente una calificación de riesgo inherente general y riesgo de control para un riesgo con varios eventos de riesgos que tienen diferentes calificaciones de riesgo inherente y riesgo de control, en función del recuento de cuántos de los eventos de riesgos están calificados alto, medio o bajo.



Fondo de mapa de calor simple

1: No proporcionar un alto nivel de integridad, transparencia y fiabilidad del servicio y la entrega de productos y garantizar una mejora continua.
2: No impedir el soborno a un funcionario con el objetivo de facilitar la expedición de licencias, permisos, certificados y otros tipos de servicios públicos.
3: Fallar en asegurar la participación de los socios de negocio a la política de tolerancia cero al soborno y la corrupción de la entidad.

En una visión alternativa y más holística, un eje denotaría calificaciones de riesgo inherentes y el otro eje denotaría calificaciones de riesgo de control. Cada evento de riesgo se trazaría en función de su riesgo inherente y su calificación o puntuación de riesgo de control. Esta vista permite a una empresa ver cómo se califica cada riesgo inherente con respecto a la efectividad de sus controles de mitigación. Bajo el modelo tradicional discutido anteriormente, la gerencia a menudo está sesgada hacia la mitigación de eventos de alto impacto y alta probabilidad. Sin embargo, si un riesgo es relevante para la empresa y tiene un impacto extremadamente alto, debe abordarse, independientemente de la probabilidad. Por lo tanto, puede ayudar a resaltar los riesgos improbables, pero potencialmente devastadores en los que la alta gerencia y los encargados del gobierno corporativo deben enfocarse (los llamados eventos *Black Swan*). La figura siguiente muestra dicho mapa de calor. Al igual que con todos los demás aspectos del proceso de evaluación de riesgos, la elección y el diseño de mapas de calor también son más efectivos si se construyen en consulta con diferentes niveles de gerencia y partes interesadas relevantes de diferentes funciones, ubicación y unidades comerciales, según corresponda. Otra consideración importante es que los riesgos a los que está expuesta la empresa cambian con el tiempo, por lo que es importante actualizar los mapas de calor de forma periódica para comprender los problemas más pertinentes en ese momento.



1: No proporcionar un alto nivel de integridad, transparencia y fiabilidad del servicio y la entrega de productos y garantizar una mejora continua.
2: No impedir el soborno a un funcionario con el objetivo de facilitar la expedición de licencias, permisos, certificados y otros tipos de servicios públicos.
3: Fallar en asegurar la participación de los socios de negocio a la política de tolerancia cero al soborno y la corrupción de la entidad.

7.8.2 Preparación de un informe resumido

El proceso de evaluación de riesgos de corrupción involucra a una variedad de partes interesadas en diferentes niveles de participación para producir la evaluación final. Si bien algunos miembros del personal pueden estar muy interesados en los detalles particulares de la evaluación, los altos ejecutivos y los encargados del gobierno corporativo pueden beneficiarse de un informe resumido. El resumen establecería de manera concisa los procedimientos seguidos, los riesgos clave identificados, los controles de mitigación clave, las brechas de control identificadas y las respuestas planificadas para abordar los riesgos residuales de manera priorizada. Este informe resumido debe ser independiente, pero también puede ayudar al lector a navegar hacia información más detallada en otra documentación.

Para lograr estos objetivos, un formato recomendado del informe resumido incluiría las siguientes secciones:

- Resumen Ejecutivo.
- Declaración de propósito y objetivos.
- Resumen del alcance de la evaluación y el nivel de tolerancia al riesgo.
- Resumen del enfoque y los pasos del trabajo.
- Lista resumida de partes interesadas y participantes.
- Áreas clave de riesgo de corrupción identificadas.
- Controles de mitigación clave.
- Identificación de brechas de control.
- Plan de respuesta.
- Agradecimientos (agradecimiento a los participantes, asesores y otros contribuyentes).
- Adjuntos.

Un resumen ejecutivo, que no debe tener más de 1 o 2 páginas, podría incluir las áreas clave de riesgo, los controles clave y los elementos clave del plan de respuesta. Además, es importante considerar incluir estadísticas clave (por ejemplo, el porcentaje total de riesgos inherentes y residuales altos versus medios versus bajos), observaciones generales, ubicaciones y unidades comerciales cubiertas por la evaluación.

También conviene considerar la posibilidad de incluir cuadros y gráficos resumidos seleccionados (como mapas de calor) que se puedan extraer de la evaluación detallada del riesgo de corrupción, como:

- Áreas de mayor riesgo inherente.
- Áreas de mayor riesgo residual.
- Áreas de alto riesgo inherente que tienen bajos riesgos residuales.
- Resumen de controles que mitigan áreas de alto riesgo inherente.
- Resultados ilustrados por proceso, unidad de negocio o ubicación.
- Gráficos de significancia versus verosimilitud.
- Gráficos de calificación de riesgo inherente versus riesgo de control.
- Gráficos de calificación de riesgo inherente versus riesgo residual.

8. PARTICIPANTES

8.1 Redactado y armado

Dr. Cdor. Claudio Borsetti
Dra. Cdora. Paula D´Onofrio

8.2 Coordinación y revisión de calidad

Dr. Cdor. Mariano J. Fernández, Vicepresidente de la Comisión Integridad y Cumplimiento.
Dr. Cdor. Raúl R. Saccani, Presidente de la Comisión Integridad y Cumplimiento.

9. BIBLIOGRAFÍA

1. AFI (2019), Sostenibilidad y Gestión de activos. Recuperado de https://www.afi.es/webAfi/descargas/1914098/1368472/Guia-practica-Sostenibilidad-y-Gestion-de-Activos-Afi-y-Allianz-Global-Investors.pdf
2. Alliance for Integrity (2017), "Pacto Global". Obtenido de http://pactoglobal.org.ar/novedades/una-app-que-te-permite-gestionar-el-10mo-principio-del-pacto-global/
3. ARGENTINA CÓDIGO PENAL (1984). http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm
4. ARGENTINA Ley 27.401. (2017), INFOLEG. Obtenido de http://servicios.infoleg.gob.ar/infolegInternet/anexos/295000-299999/296846/norma.htm
5. Asociación Argentina de Ética y Compliance (2017), *Libro Blanco sobre la función de Compliance,* Buenos Aires.
6. Borsetti, C. (2022), "Norma ISO 37001: 2016 - Sistema de Gestión Anti-Soborno Gestión proactiva de riesgos. Prácticas de modelos".
7. Borsetti, C. (2021), "ISO 37001:2016 Sistema de Gestión anticorrupción. Soluciones para asegurar su empresa".
8. Borsetti, C. (2019), "Curso de auditor interno ISO 37001:16", Intertek.
9. Borsetti, C. (2018), "Taller práctico de Mapeo de riesgos".
10. Borsetti, C. (2022), "Análisis proactivo de riesgos - Mapa de riesgos para la elaboración de un Programa de Integridad", Universidad de Belgrano.
11. Borsetti, C. (2005), "Enterprise Risk Management: Aligning Risk Management with Business Strategy", AON Consulting.
12. Borsetti, C. (2020), "AIAG & VDA FMEA 2019", Intertek.
13. Casanovas Ysla, A.(2021), *Guía práctica de compliance según la Norma ISO 37301:2021*. AENOR
14. CEPAL (2016), *Agenda 2030 y los Objetivos de Desarrollo Sostenible. Una oportunidad para América Latina y el Caribe*.
15. Coleman, T. (2012), "Una guía práctica para la gestión de riesgos" (resumen), Research Foundation of CFA Institute Monograph, https://ssrn.com/abstract=2279377 (último acceso 07/06/2023).
16. Committee of Sponsoring Organizations of Treadway Commission (COSO) y World Business Council for Sustainable Development (WBCSD).(2018) "Gestión del Riesgo Empresarial — Integrando Estrategia y Desempeño - Aplicación de la gestión del riesgo empresarial a los riesgos relacionados con factores medioambientales, sociales y de gobierno" https://cecodes.org.co/wp-content/uploads/2022/11/COSO-ESG-Espanol.pdfCOSO -WBCSD Guía para la gestión de riesgos ESG
17. Durrieu & Saccani - Directores (2018), *Compliance, Anticorrupción y Responsabilidad Penal Empresaria,* CABA, La Ley.
18. Eyharchet, C. A y Angueira, D.(2021), "El triángulo del fraude ¿Sigue vigente?".
19. Grupo de Acción Financiera de Latinoamérica GAFILAT "Estudio integral del sector de APNFD a nivel regional", septiembre. https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/estudios-estrategicos-17/4217-estudio-integral-del-sector-de-apnfd-a-nivel-regional (último acceso 07/06/2023)
20. NACIONES UNIDAS (2020) Guía de Integridad Sostenible https://pactoglobal.org.ar/novedades/integridad-sostenible-el-primer-programa-acelerador-orientado-al-ods-16-en-argentina/

21. The Financial Action Task Force (FATF)(2014) Guidance for a risk-based approach - https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf
22. Hernández Pérez, M.y García Salvador R. (2019), *Guía para la aplicación de UNE-ISO 37001:2017.*
23. CONSEJO PROFESIONAL DE CIENCIAS ECONOMICAS CABA Comisión Anticorrupción, Informe 1: *Aspectos prácticos y preguntas frecuentes en la implementación de Programas de Integridad* (2018)
24. CONSEJO PROFESIONAL DE CIENCIAS ECONOMICAS CABA (2020) Comisión Anticorrupción, Informe 2: *Guía para la implementación de programas de Integridad* https://www.consejo.org.ar/storage/attachments/InfoN%C2%BA2-Comisi%C3%B3nAnticorrupci%C3%B3n.pdf-uX4JNYvhVq.pdf
25. CONSEJO PROFESIONAL DE CIENCIAS ECONOMICAS CABA Comisión de Integridad y Cumplimiento, Informe 3: *Beneficio Indebido: Un análisis preliminar* https://archivo.consejo.org.ar/publicacionesedicon/Informe3-Beneficio-Indebido-Un-Analisis-Preliminar-Anticorrupcion.pdf - (2022)
26. ISO/IEC TS 17021-9 Requisitos de competencia para la auditoría y la certificación de sistemas de gestión antisoborno (2015), Secretaría Central de ISO en Ginebra, Suiza.
27. ISO 31000 Risk management (2015), Guidelines.
28. Kaplan, J. (2019), *Compliance & Ethics Risk Assessment: Concepts, Methods and New Directions* (Expanded Edition), Corporate Compliance Insights, Dallas, Texas.
29. Kleinhempel, M. (2021), *Los ocho pilares del compliance: reflexiones* y *propuestas*, 1ra. edición revisada, Buenos Aires, Temas Grupo Editorial.
30. Lema, A. (2021), "Riesgos empresariales: concepto, clases y métodos de análisis y evaluación", World Compliance Association.
31. Lizarzaburu Bolaños, E..; BarrIga, G.; Burneo, K.; Noriega, E. (2019)"Gestión Integral de Riesgos y Antisoborno: Un enfoque operacional desde la perspectiva ISO 31000 e ISO 37001".
32. Lopez, P., "Taller ISO 37001" (2020), World Compliance Association.
33. Preve, L. (2014), "Determinants of Risk", http://lorenzopreve.com/determinants-of-risk/ (último acceso 07/06/2023)
34. "Principles for Responsible Investment" (2005). Obtenido de www.unpri.org.
35. Saccani, Raúl (2018), *Tratado de Compliance,* Thomson Reuters La Ley.
36. UK BRIBERY ACT. (2010). https://www.gov.uk/anti-bribery-policy#:~:text=It%20is%20illegal%20to%20offer,might%20be%20exposed%20to%20bribery. Obtenido de http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-quick-start-guide.pdf
37. UNE ISO 37301 Sistema de Gestión del Compliance, Asociación Española de Normalización (2022)
38. United Nations Global Compact. (2013), *A Guide for Anti-Corruption Risk Assessment.* https://unglobalcompact.org/library/411 (último acceso 24/04/2023)
39. U.S. DEPARTMENT OF JUSTICE. (s.f.), https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act. Recuperado en julio de 2020.
40. U.S. DEPARTMENT OF JUSTICE CRIMINAL DIVISION (June 2020), https://www.justice.gov/criminal-fraud/page/file/937501/download. Obtenido de EVALUATION OF CORPORATE COMPLIANCE PROGRAM.
41. WBCSD, W. B. (2011), *Visión 2050. Una nueva agenda para las empresas,* CEADS, Ed. Recuperado el 22 de enero de 2014, de http://www.wbcsd.org/pages/edocument/edocumentdetails.aspx?id=219&nosearchcontextkey=true
42. Yordanov, N. (2018), "Intertek Proactive Risk Management Solutions for Optimizing Business Processes".
43. Yordanov, N. (2018), "ISO 37001 & ISO 17021-9 2016 ABMS", Intertek.
44. Yordanov, N. (2019), "Intertek Proactive SGAS Ejemplo de perfil de riesgo", Intertek.
45. Yordanov, N. (2018), "Proactive Risk Solutions & ISO 31000", Intertek.