Instructivo:
INS.UDC.2.2.02.01
Gestionar la evaluación de riesgos de soborno

(Referentes de la Comisión Operativa del Sistema de Gestión Antisoborno)

Junio 2025

(Referentes de la Comisión Operativa del Sistema de Gestión Antisoborno)

Introducción

La Norma Internacional ISO 37001, del Sistema de Gestión Antisoborno, es un estándar internacional que proporciona directrices y requisitos para que las organizaciones implementen medidas efectivas contra el soborno y la corrupción, los cuales son problemas persistentes en todo el mundo, que socavan la ética empresarial, distorsionan la competencia justa, perjudican el desarrollo económico y social. Es necesario utilizar la Norma ISO 37001 por varias razones fundamentales:

1) **Combatir la corrupción:** El soborno es una forma de corrupción que mina la integridad y la transparencia en los negocios. La Norma ISO 37001 ayuda a las organizaciones a prevenir, detectar y abordar el soborno de manera sistemática y efectiva, promoviendo una cultura de ética y honestidad.

2) **Cumplimiento legal y normativo:** Muchos países han implementado leyes y regulaciones para combatir el soborno, como la Ley de Prácticas Corruptas en el Extranjero (FCPA) de los Estados Unidos o la Ley de Soborno del Reino Unido. La adopción de la Norma ISO 37001 ayuda a las organizaciones a cumplir con estos requisitos legales y normativos, evitando multas, sanciones y daños reputacionales.

3) **Mejora de la reputación**: Una institución que implementa un Sistema de Gestión Antisoborno demuestra su compromiso con la integridad y la responsabilidad. Esto fortalece su reputación y genera confianza entre los clientes, los inversores y otras partes interesadas, lo que puede traducirse en ventajas competitivas y oportunidades de negocio.

4) **Gestión de riesgos:** El soborno representa un riesgo significativo para las organizaciones, que puede llevar a pérdidas financieras y daños irreparables. La Norma ISO 37001 proporciona un marco sólido para identificar, evaluar y gestionar los riesgos de soborno, permitiendo a las organizaciones tomar medidas preventivas y correctivas adecuadas.

5) **Fomento de la transparencia y la ética:** La implementación de la Norma ISO 37001 fomenta la transparencia en las operaciones comerciales y promueve una cultura de ética y cumplimiento en toda la institución. Esto no solo contribuye al éxito a largo plazo de la institución, sino que también tiene un impacto positivo en la sociedad y en el entorno empresarial en general.

En resumen, utilizar la Norma ISO 37001 es fundamental para combatir el soborno, cumplir con la legislación y los requisitos normativos, mejorar la reputación, gestionar los riesgos y fomentar la transparencia y la ética en las organizaciones. Es una herramienta efectiva para promover prácticas empresariales justas, responsables e íntegras, y contribuir al desarrollo sostenible de las empresas y las sociedades en las que operan.

Antecedentes

El antecedente principal de la Norma ISO 37001 es la Convención de las Naciones Unidas contra la Corrupción (UNCAC, por sus siglas en inglés). La UNCAC es un tratado internacional adoptado por la Asamblea General de las Naciones Unidas en 2003, con el objetivo de promover y fortalecer medidas para prevenir y combatir la corrupción a nivel global. La ISO 37001 se basa en los principios y requisitos establecidos en la UNCAC, así como en otras iniciativas internacionales relacionadas con la lucha contra el soborno y la corrupción. Estos incluyen el Manual de la OCDE para Combatir el Soborno de Funcionarios Extranjeros en Transacciones Comerciales Internacionales y la Ley de Prácticas Corruptas en el Extranjero (FCPA) de los Estados Unidos.

La necesidad de una norma internacional específica para combatir el soborno y promover la integridad empresarial se hizo evidente debido a la creciente preocupación mundial por la corrupción y su impacto negativo en los negocios y en la sociedad en general. La ISO (Institución Internacional de Normalización) reconoció esta necesidad y desarrolló la Norma ISO 37001 en respuesta a la demanda de un enfoque estandarizado y efectivo para prevenir y combatir el soborno. La Norma ISO 37001 fue publicada en octubre de 2016 y establece los requisitos para implementar un Sistema de Gestión Antisoborno en una institución. Proporciona directrices para prevenir, detectar y abordar el soborno, incluyendo políticas y procedimientos, controles internos, capacitación y comunicación, y evaluación de riesgos. Además, establece medidas para gestionar las transacciones y relaciones comerciales de manera ética y responsable.

El MINEDUCYT, en cumplimiento de su misión, en función de garantizar a la población estudiantil una educación de calidad; no está exenta de riesgos de corrupción; por lo que, la implementación de la evaluación de riesgos de soborno, constituye el primero de los esfuerzos para prevenir, detectar y gestionar los posibles casos de soborno; así como una política antisoborno y la concientización de los servidores públicos, proveedores, socios y grupos de interés para formar parte del Sistema de Gestión Antisoborno institucional.

Objetivo:

Brindar las orientaciones para realizar la autoevaluación de riesgos de soborno, basada en las mejores prácticas internacionales, que permitan la identificación, análisis, evaluación y seguimiento de potenciales riesgos de soborno que afecten la integridad del MINEDUCYT, con la finalidad de implementar un Sistema de Gestión Antisoborno.

Alcance:

La evaluación de riesgos deberá aplicarse a todas las Unidades Organizativas del MINEDUCYT; así como también implementarse en las Direcciones Departamentales de Educación y centros escolares oficiales. Este instructivo, pretende incluir elementos y criterios básicos para la identificación, análisis, evaluación, planes de acción, en respuesta al riesgo de soborno y sus variantes. Así mismo, disponer de un instrumento estándar para la aplicación a nivel institucional, que permita la consolidación, seguimiento a cada unidad organizativa del MINEDUCYT.

Indicaciones generales:

Referentes de la Comisión Operativa del Sistema de Gestión Antisoborno:

1. Informa al Director de la Unidad Organizativa sobre las actividades a realizar para la "Evaluación de Riesgos de Soborno" y conforma al equipo de evaluación de riesgos de soborno.

2. Identifica los procesos en los que participa la Unidad Organizativa en el Inventario de Procedimientos (verificar Anexo 3 del Manual de Procesos Institucionales).

3. Organiza al equipo de evaluación de riesgos de soborno de los procesos y da las orientaciones necesarias.

Referente de la Comisión Operativa del Sistema de Gestión Antisoborno: y equipo de evaluación de riesgos de la Unidad Organizativa:

4. Revisa la Ficha de los Procesos y verifica en la matriz SIPOC los principales procedimientos con mayor exposición a riesgos de soborno, y aplica la metodología para la evaluación de riesgos de soborno y realiza el registro correspondiente en la plataforma. (Según materiales de apoyo)

5. Notifica por correo electrónico a la Dirección de Planificación, adjuntando la lista de participantes, y captura de pantalla del registro en la plataforma.

Unidad de Cumplimiento:

6. Realiza el seguimiento a los resultados de la evaluación de riesgos de soborno.

7. Elabora y presenta informe consolidado y Plan de Acción de mejora a la Comisión Estratégica del Sistema de Gestión Antisoborno y a los Titulares.

Principales Definiciones

- **Conflicto de intereses:** Situación donde los intereses de negocios, financieros, familiares, políticos o personales podrían interferir con el juicio de valor del personal en el desempeño de sus obligaciones hacia la organización.

- **Evaluación de riesgo:** Es un proceso sistemático que consiste en identificar, analizar y evaluar los riesgos potenciales asociados con una actividad, proyecto o situación. La evaluación de riesgo tiene como objetivo principal determinar la probabilidad de ocurrencia de un riesgo y evaluar el impacto que este riesgo podría tener en los objetivos, recursos o activos de una institución.

- **Impacto:** *Es el conjunto de consecuencias que origina un riesgo si llegará a presentarse.*

- **Norma ISO 37001:** Es un estándar internacional desarrollado por la Institución Internacional de Normalización (ISO) que establece los requisitos para un Sistema de Gestión Antisoborno (SGA). Fue publicada en octubre de 2016 y tiene como objetivo proporcionar a las organizaciones una guía para prevenir, detectar y abordar el soborno en todas sus formas.

- **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan, que transforma los elementos de entrada en elementos de salida.

- ***Probabilidad:*** *Es la posibilidad de que ocurra un riesgo, tomando en cuenta los controles actuales y su efectividad.*

- **Riesgo:** Efecto de la incertidumbre en los objetivos. Se define también, como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas.

- **Riesgo de integridad:** Se refiere a la posibilidad de que una institución o individuo se involucre en comportamientos o acciones que violen los principios éticos, la transparencia y los valores de integridad. Este riesgo implica la amenaza de conductas inapropiadas, como fraude, corrupción, conflicto de intereses, malversación de fondos, comportamiento antiético y otras actividades ilícitas que pueden dañar la reputación y la credibilidad de una institución.

- **Sistema de Gestión Antisoborno (SGA):** Es un conjunto de políticas, procedimientos, controles y prácticas establecidos por una institución para prevenir, detectar y abordar el soborno en todas sus formas. El SGA proporciona un marco estructurado para que las organizaciones promuevan una cultura de integridad, transparencia y ética en sus actividades y relaciones comerciales.

- **Soborno:** Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directamente o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona.

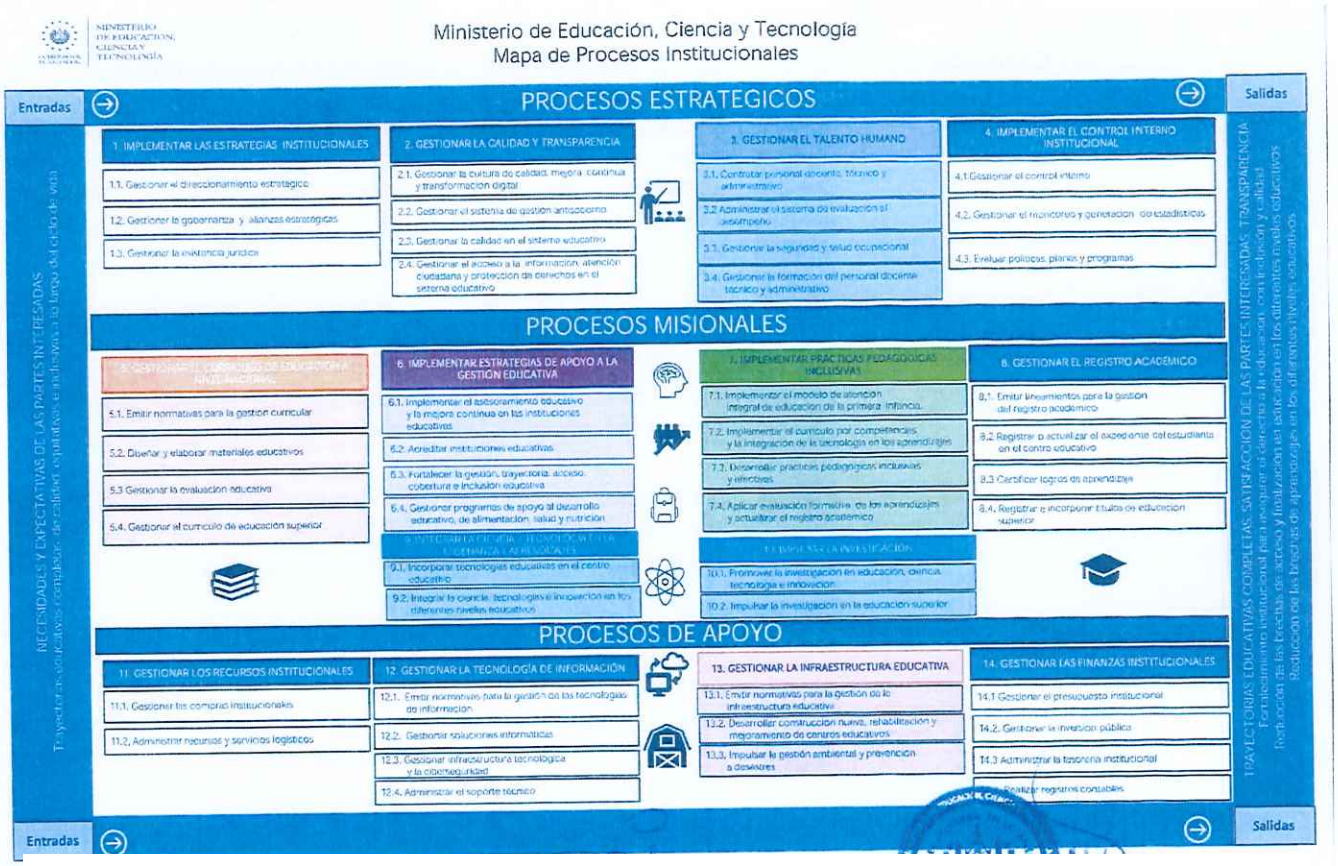
EVALUACIÓN DEL RIESGO DE SOBORNO

1. IDENTIFICACIÓN

En esta etapa, se identifican los posibles riesgos de soborno a los que está expuesta una institución. Esto implica analizar, comprender las actividades, procesos, operaciones y contextos en los que opera la institución, así como los posibles eventos o circunstancias que podrían generar riesgos. Se pueden utilizar técnicas como entrevistas, revisión documental, listas de verificación y análisis de datos históricos para identificar los riesgos potenciales.

1.1. Procesos y Sub-Procesos Institucionales

Se ha definido Procesos y Sub-Procesos estratégicos que enmarcan todas las actividades de las unidades organizativas que conforman el MINEDUCYT en el Mapa de Procesos Institucionales, autorizado el 10 de abril de 2025. Información que se puede consultar con más detalle en el Manual de Procesos Institucionales, el cual será remitido por la Dirección de Planificación y publicado en el Portal de Calidad.



1.2. **Descripción de los Riesgos:** Consiste en la descripción de los principales riesgos que atenten contra la integridad del MINEDUCYT, los cuales constituyen comportamiento o acciones que violentan los principios éticos, la transparencia y los valores de integridad. Al establecer los riesgos se debe ser concreto, claro y preciso, para que sea entendible para cualquiera que los vea, incluyendo al personal relacionado con las acciones para minimizarlos y quienes hacen el monitoreo general del Sistema de Gestión Antisoborno.

1.3. **Ámbito del Riesgo:** Los riesgos pueden tener asociado un factor de origen interno o externo, lo cual es importante definir, para establecer las estrategias adecuadas para su tratamiento.

1.4. **Tipo de Riesgo:** Existen varios tipos de riesgos de soborno que se pueden presentar en el MINEDUCYT. Estos riesgos pueden variar según las funciones específicas que le corresponden a cada una de las unidades organizativas. A continuación, se presentan algunos de los tipos más comunes de riesgos de soborno:

TIPO DE RIESGO	DESCRIPCIÓN
Corrupción	Se refiere a prácticas o comportamientos deshonestos e ilegales en los que los individuos abusan de su poder o posición de autoridad en beneficio personal o para obtener ventajas indebidas. Es un fenómeno complejo que afecta a diversos sectores y niveles de la sociedad, y puede tener consecuencias negativas significativas tanto a nivel económico como social.
Soborno en contratos o convenios	Este riesgo implica la corrupción en procesos de licitación y adjudicación de contratos o convenios. Puede incluir el pago de sobornos a funcionarios públicos o a empleados de otras empresas con el fin de obtener una ventaja indebida en la competencia por contratos o convenios.
Soborno a funcionarios	Este riesgo se refiere a la corrupción de funcionarios públicos, ya sea para obtener favores, influir en decisiones gubernamentales o asegurar contratos y permisos.
Soborno a empleados	Se refiere a la práctica de ofrecer, entregar, solicitar o aceptar pagos, regalos, beneficios u otros incentivos ilícitos con el fin de influir en las decisiones o acciones de los empleados de una institución. Es una forma de corrupción que implica el uso indebido de poder o posición para obtener ventajas personales o beneficios indebidos.
Conflicto de intereses	Situación en la cual los intereses personales o financieros de un individuo entran en conflicto con los intereses de la institución para la cual trabaja. Este conflicto puede afectar la objetividad, imparcialidad y toma de decisiones justas del individuo, lo que puede comprometer la integridad y la confianza en la institución.
Extorsión y chantaje	Estos riesgos implican la amenaza de daño o perjuicio al MINEDUCYT, sus empleados o sus intereses, con el objetivo de obtener beneficios financieros o favores indebidos. La extorsión y el chantaje pueden provenir tanto de actores internos como externos a la institución.

Donaciones y contribuciones indebidas	Este riesgo se refiere a la utilización de donaciones, contribuciones políticas o caridad como fachada para encubrir el soborno. Puede implicar el uso indebido de fondos de la institución para influir en decisiones políticas o asegurar beneficios comerciales indebidos.
Soborno por intermediarios	Muchas organizaciones utilizan intermediarios, como agentes, consultores o distribuidores, para realizar transacciones comerciales. Sin embargo, existe el riesgo de que estos intermediarios actúen de manera corrupta, pagando sobornos en nombre de la institución para obtener beneficios indebidos.
Lavado de dinero	El riesgo de lavado de dinero está estrechamente relacionado con el soborno. Las organizaciones pueden verse involucradas en actividades de lavado de dinero al recibir y ocultar ganancias ilícitas generadas a través de sobornos. El lavado de dinero implica la transformación de dinero ilegal en apariencia de legítimo.

1.5. **Clasificación de Riesgo:** Una vez identificado el tipo de riesgo, se debe definirla clasificación del mismo, ya que de materializarse la situación prevista es importante conocer qué área sería la principalmente afectada.

CLASE DE RIESGO	DESCRIPCIÓN
Financiero	Representan la posibilidad de obtener detrimentos económicos en los activos o recursos institucionales.
Operativo	Consiste en posibles alteraciones en la gestión, relacionadas con el manejo inadecuado o fallido de aspectos organizacionales por parte de los servidores públicos.
Estratégico	Se refiere a la ocurrencia de acontecimientos que afecten directamente la misión y visión institucional.
Legal (Cumplimiento)	Se refieren a la posibilidad de que una entidad tenga o se vea afectada por incumplir u omitir ciertas leyes, regulaciones o políticas internas.
A la Integridad	Está relacionado con la posibilidad de que un servidor público actúe de modo voluntario para obtener un beneficio propio en detrimento de la ciudadanía.
Tecnológico	Consiste en la posibilidad de que alguna herramienta tecnológica falle o sea utilizada inadecuadamente en detrimento de los fines institucionales.

Servicios Educativos	Está relacionado con la posibilidad que los servicios educativos no sean brindados con calidad a la población estudiantil. En este caso se entiende tanto los servicios educativos directos, como también todos los programas educativos destinados a mejorar las condiciones de los estudiantes, docentes y centros educativos.
Reputacional (Imagen)	Se refiere al desprestigio de la entidad por la ocurrencia de actos de corrupción que trae como consecuencia la pérdida de credibilidad y confianza de la sociedad.

2. ANÁLISIS

Una vez que se han identificado los riesgos, se procede a analizarlos en términos de su probabilidad de ocurrencia y su impacto potencial. Esto implica evaluar la posibilidad de que ocurra un riesgo y comprender las consecuencias negativas asociadas si se materializa. El análisis de riesgos puede basarse en datos históricos, estadísticas, juicio experto y evaluación de la magnitud del impacto.

2.1. **Causas del Evento:** La causa de un riesgo se refiere a la circunstancia o factor que puede generar la materialización de un evento o situación no deseada que tiene el potencial de causar daños, pérdidas o impactos negativos en la consecución de los objetivos del MINEDUCYT. Los riesgos pueden tener diversas causas, y su origen puede variar según el contexto y la naturaleza de las actividades realizadas en cada unidad organizativa. Estos pueden proceder de factores internos o externos. Las causas de riesgo pueden ser diversas y variar según el contexto. Algunos ejemplos comunes de causas de riesgo incluyen:

Fallos en los sistemas o procesos	Errores, interrupciones, deficiencias o mal funcionamiento en los sistemas tecnológicos, administrativos o procedimentales que impiden el desarrollo eficiente, oportuno y correcto de las actividades y servicios educativos o institucionales.
Factores humanos	Las acciones, decisiones, omisiones, actitudes o comportamientos del personal (docentes, administrativos, directivos, técnicos, etc.) que pueden influir positiva o negativamente en el desarrollo de los procesos institucionales, la prestación de servicios educativos y el logro de los objetivos organizacionales.
Riesgos tecnológicos	Amenazas, vulnerabilidades o fallos relacionados con el uso, implementación o dependencia de tecnologías de la información y comunicación (TIC), que pueden afectar la continuidad, seguridad, eficiencia o calidad de los servicios y procesos educativos o administrativos.
Procesos no normados	Actividades, procedimientos o prácticas que se realizan sin estar formalmente documentadas, reguladas o respaldadas por normativas institucionales, lo que puede generar riesgos de ineficiencia, inconsistencia, falta de control o incumplimiento legal.
Normativa desactualizada	Reglamentos, políticas, manuales, lineamientos o procedimientos institucionales que ya no responden a las necesidades actuales, cambios legales, tecnológicos o contextuales, y que, por tanto, dificultan una gestión eficaz, eficiente y conforme a la realidad vigente.

Cambios en políticas públicas	Modificaciones, ajustes o transformaciones en las directrices, planes, prioridades o estrategias establecidas por el gobierno en materia educativa, que pueden impactar directa o indirectamente en la planificación, ejecución y evaluación de los programas, servicios y recursos del sistema educativo.

2.2. **Consecuencias o Efectos Potenciales:** Las consecuencias de un riesgo se refieren a los resultados o impactos negativos que pueden ocurrir si un evento o situación de riesgo se materializa. Estas consecuencias pueden afectar la consecución de los objetivos institucionales, y pueden tener diversas manifestaciones en términos de pérdidas, daños, interrupciones, costos adicionales u otros efectos indeseables. Las consecuencias de los riesgos pueden variar según el tipo de riesgo y el contexto específico, pero algunas de las consecuencias comunes incluyen:

Detrimento de fondos	Pérdida, mal uso o daño económico que afecta a los recursos financieros de una institución, entidad pública o privada. Es decir, cuando los fondos o dineros disponibles se ven disminuidos o comprometidos negativamente, ya sea por: mala administración, uso indebido, corrupción, pagos injustificados, errores contables o de gestión, o cualquier otra causa que genere un perjuicio económico.
Interrupción de las operaciones	La suspensión total o parcial, temporal o prolongada, de los procesos, actividades o servicios esenciales para garantizar el funcionamiento del sistema educativo.
Litigios y responsabilidad legal	Se refiere a los procesos judiciales, demandas o procedimientos legales en los que la institución se ve involucrada, ya sea como demandante o demandado, y a las obligaciones legales que pueden surgir como resultado de estos casos, incluyendo sanciones, indemnizaciones o cumplimiento de fallos judiciales.
Servicios no proporcionados	La falta de entrega, cumplimiento o ejecución total o parcial de servicios que el MINEDUCYT, o sus dependencias están obligados a brindar, ya sea por contrato, programación institucional o mandato legal, afectando así el acceso, la calidad o la continuidad del servicio educativo.

2.3. **Controles Existentes:** Para completar el análisis de los riesgos, es importante, validar si existen controles previos que mitiguen las situaciones determinadas. La existencia de estos, no implican que sean los más adecuados de acuerdo con las circunstancias; por tanto, es recomendable actualizarlos como parte del plan de acción que se considera más adelante.

Tipo de controles con base en la Norma ISO 37001:2016 Sistema de Gestión Antisoborno (criterio 8):

8.1 Planificación y control operacional	La organización debe planificar, implementar, revisar y controlar los procesos necesarios para cumplir los requisitos del Sistema de Gestión Antisoborno y para implementar las acciones determinadas en 6.1, mediante: a) El establecimiento de criterios para los procesos; b) La implementación del control de los procesos de acuerdo con los criterios; c) Manteniendo información documentada en la medida necesaria para confiar en que los procesos se han llevado a cabo según lo planificado.

Estos procesos deben incluir los controles específicos mencionados en los apartados 8.2 a 8.10. La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar cualquier efecto adverso, según sea necesario.

8.2 Debida diligencia

Cuando la evaluación del riesgo de soborno de la organización llevada a cabo en 4.5, ha evaluado más que un riesgo bajo de soborno en relación con:
a) Determinadas categorías de transacciones, proyectos o actividades,
b) Las relaciones existentes o planificadas con determinadas categorías de socios de negocios; o
c) Categorías específicas del personal en determinadas posiciones.
(véase 7.2.2.2).
La organización debe evaluar la naturaleza y el alcance del riesgo de soborno en relación a transacciones, proyectos, actividades, socios de negocios y el personal, pertenecientes a estas categorías específicas. Esta evaluación debe incluir cualquier debida diligencia necesaria para obtener información suficiente para evaluar el riesgo de soborno. La debida diligencia debe actualizarse con una frecuencia definida para que los cambios y la nueva información pueda tenerse en cuenta debidamente.

8.3 Controles financieros

La organización debe implementar controles financieros que gestionen el riesgo de soborno.

8.4 Controles no financieros

La organización debe implementar controles no financieros para gestionar el riesgo de soborno en áreas tales como compras, ventas, comercial, recursos humanos, actividades legales y reglamentarias.

8.5 Implementación de los controles antisoborno por organizaciones controladas y por socios de negocios

8.5.1 La organización debe implementar procedimientos que requieran que todas las demás organizaciones sobre las que tiene control, bien:
a) Implementen el sistema de gestión antisoborno de la organización; o bien
b) Implementen sus propios controles antisoborno, en cada caso, solo en la medida en que sea razonable y proporcional, en relación con los riesgos de soborno a los que se enfrentan las organizaciones controladas, teniendo en cuenta la evaluación del riesgo de soborno realizada de conformidad con el apartado 4.5.

8.5.2 En relación con los socios de negocios no controlados por la organización para los que la evaluación del riesgo de soborno (véase 4.5) o la debida diligencia (véase 8.2) han identificado más que un riesgo bajo de soborno, y donde los controles antisoborno implementados por los socios de negocios ayudarían a mitigar el riesgo de soborno relevante, la organización debe implementar procedimientos de la siguiente manera: a) la organización debe determinar si el socio de negocios tiene implementados controles antisoborno que gestionan el riesgo relevante de soborno; b) donde un socio de negocios no tiene en marcha controles antisoborno, o no es posible verificar si los tiene implementados:

1) donde sea posible, la organización debe exigir al socio de negocios la implementación de controles antisoborno en relación con la transacción, proyecto o actividad correspondiente, o

2) donde no es posible exigir al socio de negocios implementar controles antisoborno, esto debe ser un factor que se tome en cuenta al evaluar el

riesgo de soborno de la relación con este socio de negocio, y la forma en que la organización gestionan dichos riesgos…

8.6 Compromisos antisobornos

Para socios de negocios que representan más que un riesgo bajo de soborno, la organización debe implementar procedimientos que exijan, en la medida de lo posible, que:

a) Los socios de negocios se comprometan a prevenir el soborno por, o en nombre de, o en beneficio del socio de negocios en relación con la transacción, proyecto, actividad o relación correspondiente;
b) La organización sea capaz de poner fin a la relación con el socio de negocios en el caso de soborno por parte de, o en nombre de, o en beneficio del socio de negocios en relación con la transacción, proyecto, actividad o relación correspondiente.
Cuando no sea posible cumplir los requisitos anteriores a) o b), este debe ser un factor a tener en cuenta para evaluar el riesgo de soborno de la relación con este socio de negocios.

8.7 Regalos, hospitalidad, donaciones y beneficios similares

La organización debe implementar procedimientos que estén diseñados para prevenir la oferta, el suministro o la aceptación de regalos, hospitalidad, donaciones y beneficios similares, en los que la oferta, el suministro o la aceptación son o razonablemente podrían percibirse como soborno.

8.8 Gestión de los controles antisoborno inadecuados

Cuando la debida diligencia (véase 8.2) realizada en una transacción, proyecto, actividad o relación específica, con un socio de negocios, establece que los riesgos de soborno no pueden ser gestionados por los controles antisoborno existentes, y la organización no puede o no desea implementar controles antisoborno, mejores, adicionales o tomar medidas adecuadas (tales como cambiar la naturaleza de la transacción, proyecto, actividad o relación) para permitir a la organización gestionar los riesgos de soborno pertinentes, la organización debe:

a) En el caso de una transacción, proyecto, actividad o relación existente, adoptar las medidas adecuadas a los riesgos de soborno y la naturaleza de la transacción, proyecto, actividad o relación para terminar, interrumpir, suspender o retirarse de esto tan pronto como sea posible;

b) En el caso de una nueva propuesta de transacción, proyecto, actividad o relación, posponer o negarse a continuar con ella.

8.9 Planteamiento de inquietudes

La organización debe implementar procedimientos, para:

a) Fomentar y facilitar que las personas reporten, de buena fe o sobre la base de una creencia razonable, el intento de soborno, supuesto o real, o cualquier violación o debilidad en el sistema de gestión antisoborno, a la función de cumplimiento antisoborno o al personal apropiado (ya sea directamente o a través de una tercera parte apropiada);

b) Salvo en la medida requerida para el avance de una investigación, solicitar que la organización trate los informes de forma confidencial con el fin de proteger la identidad del informante y otras personas que participen o a las que se haga referencia en el informe;

c) Permitir la denuncia anónima;

d) Prohibir represalias, y proteger a los que realicen el reporte de represalias, después de que ellos, de buena fe o sobre la base de una creencia razonable, hayan planteado o reportado el intento de soborno, supuesto o real o violaciones de la política antisoborno o del sistema de gestión antisoborno;

e) Permitir que el personal reciba el asesoramiento de una persona apropiada sobre qué hacer si se enfrentan a un problema o situación que podría involucrar el soborno.

La organización debe asegurarse de que todo el personal esté al tanto de los procedimientos de reporte, y que sean capaces de utilizarlos, y tomen conciencia de sus derechos y protecciones de conformidad con los procedimientos.

8.10 Investigar y abordar el soborno

La organización debe implementar procedimientos para:

a) Requerir una evaluación y, cuando sea apropiado, la investigación de cualquier soborno, o el incumplimiento de la política de antisoborno o el sistema de gestión antisoborno, que haya sido informado, detectado o bajo razonable sospecha;

b) Requerir medidas apropiadas en caso de que la investigación revele algún soborno, o el incumplimiento de la política antisoborno o del sistema de gestión antisoborno;

c) Empoderar y facilitar a los investigadores;

d) Requerir la cooperación en la investigación del personal pertinente;

e) Requerir que el estado y los resultados de la investigación sean reportados a la función de cumplimiento antisoborno y a otras funciones de cumplimiento, según corresponda;

f) Requerir que la investigación se lleve a cabo de forma confidencial y que los resultados sean confidenciales.

La investigación debe ser llevada a cabo en forma confidencial y reportada por el personal que no forma parte del rol o función que está siendo investigado. La organización puede nombrar a un socio de negocio para llevar a cabo la investigación e informar de los resultados a los miembros del personal que no formen parte del papel, rol o función que están siendo investigados.

3. EVALUACIÓN

En esta etapa, se evalúa la significancia de cada riesgo identificado. Esto implica clasificar los riesgos en función de su probabilidad e impacto, y determinar cuáles son los más críticos o prioritarios para la institución. La evaluación de riesgos puede basarse en una matriz de riesgos que combine la probabilidad y el impacto para asignar una clasificación de riesgo a cada uno.

3.1. Probabilidad

Para determinar la probabilidad de materialización de los riesgos (considerando los factores y su frecuencia), después de evaluar los riesgos por su grado de impacto, debe valorarse la posibilidad de ocurrencia de acuerdo con la siguiente categoría.

Puntuación	Categoría de Probabilidad	Descripción
1	**Improbable**	Riesgo cuya probabilidad de ocurrencia es muy baja; es decir, se tiene entre 1% a 25% de seguridad que éste se presente.
2	**Remoto**	Riesgo cuya probabilidad de ocurrencia es baja; es decir, se tiene entre 25% a 50% de seguridad que éste se presente.
3	**Posible**	Riesgo cuya probabilidad de ocurrencia es media; es decir, se tiene entre 51% a 74% de seguridad que éste se presente.
4	**Muy Probable**	Riesgo cuya probabilidad de ocurrencia es alta; es decir, se tiene entre 75% a 95% de seguridad que éste se presente.
5	**Casi Seguro**	Riesgo cuya probabilidad de ocurrencia es muy alta; es decir, se tiene plena seguridad que éste se presente, tiende al 100%.

3.2. Impacto

El impacto de los riesgos se refiere a la medida en que un evento o situación de riesgo puede afectar negativamente a una institución, proyecto o actividad. El impacto está relacionado con las consecuencias y los efectos que se producirán si el riesgo se materializa.

Puntuación	Categoría de Impacto	Descripción
1	Insignificante	Riesgo que puede tener un pequeño o nulo efecto en el cumplimiento de los objetivos de la Entidad
2	Menor	Riesgo que causa un daño en el patrimonio o imagen, que se puede corregir en el corto tiempo y que no afecta el cumplimiento de los objetivos estratégicos
3	Moderado	Riesgo cuya materialización causaría una pérdida en el patrimonio o un deterioro en la imagen.
4	Mayor	Riesgo cuya materialización dañaría significativamente el patrimonio, imagen o logro de los objetivos estratégicos. Además, se requeriría una cantidad de tiempo de la Entidad en investigar y corregir los daños
5	Catastrófico	Riesgo cuya materialización influye directamente en el cumplimiento de la misión, provoca pérdida patrimonial o deterioro de la imagen, y deja además sin funciones totalmente o por un periodo importante de tiempo, los programas o servicios institucionales.

3.3. Nivel de Riesgo

Los niveles de riesgo se utilizan para evaluar, clasificar la magnitud, la importancia de un riesgo en función de su probabilidad de ocurrencia y su impacto potencial. Los niveles de riesgo pueden variar según el enfoque y la metodología utilizada, pero a menudo se utilizan categorías como las siguientes:

- Bajo riesgo: Se refiere a los riesgos con una probabilidad baja de ocurrencia y un impacto potencial mínimo o insignificante. Estos riesgos generalmente no requieren una atención prioritaria y pueden ser manejados mediante controles estándar o medidas de mitigación básicas.

- Riesgo Moderado: Se refiere a los riesgos con una probabilidad moderada de ocurrencia y un impacto potencial significativo, pero que aún se considera manejable. Estos riesgos requieren una atención adecuada y pueden necesitar controles adicionales o medidas de mitigación para reducir su impacto.

- Riesgo Alto: Se refiere a los riesgos con una probabilidad relativamente alta de ocurrencia y un impacto potencial significativo o grave. Estos riesgos requieren una atención inmediata y acciones de gestión proactivas. Se deben implementar controles sólidos y medidas de mitigación para reducir la probabilidad y el impacto de estos riesgos.

- Riesgo Extremo: Se refiere a los riesgos con una probabilidad muy alta de ocurrencia y un impacto potencial extremadamente grave. Estos riesgos representan una amenaza significativa para la institución y requieren una atención inmediata y acciones de gestión urgentes. Se deben implementar medidas exhaustivas de control y mitigación para minimizar el riesgo.

El nivel de riesgo, se representa según la siguiente escala:

NIVEL DE RIESGO		Color
B:	Riesgo Bajo	
M:	Riesgo Moderado	
A:	Riesgo Alto	
E:	Riesgo Extremo	

El mapa de riesgos, considerando los factores de "Probabilidad" e "Impacto", es el siguiente:

	Escala Cuantitativa		1	2	3	4	5
	RIESGO		IMPACTO				
			Insignificante	Menor	Moderado	Mayor	Catastrófico
5	PROBABILIDAD	Muy Probable	M	A	E	E	E
4		Alta Probabilidad	B	M	A	E	E
3		Mediamente Probable	B	M	A	A	E
2		Remoto	B	B	M	M	A
1		Improbable	B	B	B	B	M

4. PLAN DE ACCIÓN

En esta etapa, se desarrolla un plan de acción para abordar los riesgos identificados. Esto implica identificar, seleccionar estrategias para tratar cada riesgo, que pueden incluir medidas de prevención, mitigación, transferencia o aceptación del riesgo. El plan de respuesta al riesgo debe establecer claramente las acciones a seguir, los responsables, los plazos y los recursos necesarios.

4.1. Respuesta al Riesgo

La respuesta al riesgo se refiere a las acciones y medidas tomadas por la unidad organizativa para abordar, gestionar los riesgos identificados. La respuesta al riesgo implica la planificación, implementación y monitoreo de estrategias y acciones para prevenir, mitigar, transferir o aceptar los riesgos, con el objetivo de reducir su probabilidad de ocurrencia o minimizar su impacto negativo.

Las respuestas al riesgo pueden variar según la naturaleza del riesgo, el contexto y los recursos disponibles, pero generalmente se pueden clasificar en las siguientes categorías:

1) **Evitar o eliminar el riesgo:** Esta estrategia implica tomar medidas para eliminar o evitar completamente el riesgo. Esto puede implicar evitar ciertas actividades o situaciones que puedan exponer a la institución al riesgo, como rechazar ciertos proyectos o actividades que se consideren demasiado riesgosos.

2) **Reducir o mitigar el riesgo:** La mitigación del riesgo implica tomar medidas para reducir la probabilidad de ocurrencia o minimizar el impacto de un riesgo. Esto puede incluir la implementación de controles, salvaguardas adicionales, la mejora de los procedimientos operativos, el fortalecimiento de la capacitación, conciencia del personal, y la adopción de tecnologías o prácticas de trabajo más seguras.

3) **Transferir o Compartir el riesgo:** La transferencia del riesgo implica trasladar parte o la totalidad del riesgo a otra parte, como una compañía de seguros o un proveedor externo. Esto se logra a través de acuerdos contractuales o seguros que transfieren la responsabilidad de las consecuencias del riesgo a otra entidad. Así mismo, se puede considerar dentro de estos la tercerización de actividades, como la ejecución de programas por parte de socios estratégicos.

4) **Compartir el riesgo:** Se refiere a distribuir el riesgo y las posibles consecuencias, también se puede entender como transferencias parciales, en las que el objetivo no es desligarse completamente, sino segmentarlo y canalizarlo a diferentes áreas o personas, las cuales se responsabilizan de la parte del riesgo que les corresponde.

5) **Aceptar o retener el riesgo:** Se puede optar por aceptar y asumir el riesgo, especialmente cuando los costos de mitigación o transferencia del riesgo son excesivos o no factibles. Sin embargo, al asumir el riesgo, es importante establecer planes de contingencia y estar preparado para responder adecuadamente si el riesgo se materializa.

4.2. **Acciones a Implementar:** una vez se ha determinado qué respuesta al riesgo se considerará por parte de la unidad organizativa, se debe listar las acciones concretas a realizar para el cumplimiento de la misma. Estas acciones, pueden incluir trabajar en conjunto con otra unidad organizativa, para lo cual se debe realizar las coordinaciones respectivas.

4.3. **Responsables de las Acciones:** la única manera de atender efectivamente los riesgos relevantes es con acciones específicas bajo la responsabilidad de los servidores públicos que dirigen la unidad organizativa respectiva. Este individuo debe ser capaz de describir los controles existentes que responden al riesgo, discernir si los controles existentes están bien diseñados y, en su caso, definir las actualizaciones pertinentes para contar con un control efectivo.

4.4. **Período de Supervisión:** las actividades de supervisión permiten identificar y analizar las posibles brechas en el sistema de gestión de riesgo de soborno institucional comúnmente relacionadas con la presencia de anomalías o datos inusuales en la organización.

REGISTRO DE MODIFICACIONES

No.	Modificación	Fecha

Fin

GOBIERNO DE
EL SALVADOR

MINISTERIO
DE EDUCACIÓN