LICENCIA DE USO DOCUMENTOS NORMATIVOS INEN

Estos documentos se encuentran registrados CON LICENCIA DE USO, POR INEN,
AUTORIZACIÓN A USUARIO ÚNICO, PROHIBIDA SU REPRODUCCIÓN.

Esta licencia de uso debe ser leída cada vez que usted realice una compra de cualquier documento normativo suministrado por INEN, la utilización y descarga de cada documento incluye la aceptación de los términos y condiciones de esta licencia de uso.

1. El usuario de los documentos normativos tendrá la obligación de adquirir todas las medidas necesarias para evitar que personas no autorizadas tengan acceso a los documentos normativos contemplados en la licencia de uso, estas medidas deberán asegurar la confidencialidad y propiedad intelectual de los documentos normativos.
2. El usuario del o los documentos normativos no deberá distribuir, vender, ceder la licencia de uso de los documentos normativos a una tercera parte.
3. Los documentos normativos no podrán tener acceso directo a una página WEB para el libre acceso.
4. El usuario podrá imprimir los documentos normativos para el uso interno y exclusivo, el contenido total o parte de los mismos deberán mantenerse sin ningún tipo de modificación, las marcas e indicaciones de la licencia de uso no deberán ser alteradas.
5. El usuario notificará por escrito mediante correo electrónico al Servicio Ecuatoriano de Normalización – INEN (ventanormas@normalizacion.gob.ec) dentro de un plazo de treinta días naturales siguientes a la recepción de los documentos normativos, cualquier error o defecto detectado en el formato adquirido (impreso, digital), caso contrario se asumirá que el usuario se encuentra a satisfacción con la información obtenida.
6. El incumplimiento de los términos referenciados en este documento por parte del usuario será considerada una infracción a la propiedad intelectual, si INEN detectara alguna inobservancia referente a los términos de esta licencia remitirá un comunicado por escrito según corresponda.

Usted reconoce que ha dado lectura a los términos de esta licencia de uso y acuerda respetar los mismos.

Servicio Ecuatoriano de Normalización
Quito – Ecuador

NORMA
TÉCNICA
ECUATORIANA

NTE INEN-ISO 37001

Segunda edición
2025-09

SISTEMAS DE GESTIÓN ANTISOBORNO — REQUISITOS CON ORIENTACIÓN PARA SU USO (ISO 37001:2025, IDT)

ANTI-BRIBERY MANAGEMENT SYSTEMS — REQUIREMENTS WITH GUIDANCE FOR USE (ISO 37001:2025, IDT)

Correspondencia:

Esta Norma Técnica Ecuatoriana es una adopción idéntica de la traducción oficial de la Norma Internacional ISO 37001:2025.

ICS: 03.100.02; 03.100.01;03.100.70

47
Páginas

Prólogo nacional

Esta Norma Técnica Ecuatoriana NTE INEN-ISO 37001 es una adopción idéntica de la traducción oficial al español de la Norma Internacional ISO 37001:2025, *Anti-bribery management systems — Requirements with guidance for use.* El comité nacional responsable de la adopción idéntica de esta Norma Internacional es el Comité Interno del INEN.

Esta NTE INEN-ISO 37001:2025 reemplaza a la NTE INEN ISO 37001:2016.

Para el propósito de esta Norma Técnica Ecuatoriana, se indica que en la Norma Internacional ISO 37001:2025 no existen documentos normativos de referencia

Norma internacional

ISO 37001

Segunda edición
2025-02

Sistemas de gestión antisoborno — Requisitos con orientación para su uso

Anti-bribery management systems — Requirements with guidance for use

Publicado por la Secretaría Central de ISO en Ginebra, Suiza, como traducción oficial en español avalada por el *Translation Management Group*, que ha certificado la conformidad en relación con las versiones inglesa y francesa.

Número de referencia
ISO 37001:2025(es)

DOCUMENTO PROTEGIDO POR COPYRIGHT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Publicado en Suiza
Versión en español publicada en 2025

Traducción oficial

Índice

Página

Prólogo

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de elaboración de las Normas Internacionales se lleva a cabo normalmente a través de los comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho de estar representado en dicho comité. Las organizaciones internacionales, gubernamentales y no gubernamentales, vinculadas con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todos los temas de normalización electrotécnica.

En la Parte 1 de las Directivas ISO/IEC se describen los procedimientos utilizados para desarrollar este documento y aquellos previstos para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO. Este documento ha sido redactado de acuerdo con las reglas editoriales de la Parte 2 de las Directivas ISO/IEC (véase www.iso.org/directives).

ISO llama la atención sobre la posibilidad de que la implementación de este documento pueda conllevar el uso de una o varias patentes. ISO no se posiciona respecto a la evidencia, validez o aplicabilidad de los derechos de patente reivindicados. A la fecha de publicación de este documento, ISO no había recibido notificación de que una o varias patentes pudieran ser necesarias para su implementación. No obstante, se advierte a los usuarios que esta puede no ser la información más reciente, la cual puede obtenerse de la base de datos de patentes disponible en www.iso.org/patents. ISO no será responsable de la identificación de parte o la totalidad de dichos derechos de patente.

Cualquier nombre comercial utilizado en este documento es información que se proporciona para comodidad del usuario y no constituye una recomendación.

Para una explicación de la naturaleza voluntaria de las normas, el significado de los términos específicos de ISO y las expresiones relacionadas con la evaluación de la conformidad, así como la información acerca de la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) respecto a los Obstáculos Técnicos al Comercio (OTC), véase www.iso.org/iso/foreword.html.

Este documento ha sido elaborado por el Comité Técnico ISO/TC 309, *Gobernanza de las organizaciones*.

Esta segunda edición anula y sustituye a la primera edición (ISO 37001:2016) que ha sido revisada técnicamente. También incorpora la Modificación ISO 37001:2016/Amd 1:2024.

Los cambios principales en comparación con la edición previa son los siguientes:

— se añadieron apartados sobre el cambio climático y destacando la importancia de la cultura del *compliance*;

— se abordaron los conflictos de interés;

— se aclaró el concepto de función antisoborno;

— la redacción se armonizó con otras normas cuando fue apropiado y razonable;

— se introdujo la última estructura armonizada.

Términos de licencia y uso

Las publicaciones de ISO se proporcionan en virtud de diferentes tipos de acuerdos de licencia («Tipo de licencia») que permiten un derecho no exclusivo, intransferible, limitado y revocable de uso/acceso a las publicaciones de ISO para uno o más de los siguientes fines descritos a continuación («Propósito»), que pueden ser de ámbito interno o externo. El propósito o propósitos aplicables han de constar en el contrato de licencia.

a) Tipo de licencia:

   i) una única licencia de usuario final registrada (con marca de agua a nombre del usuario) para el Propósito especificado. Bajo esta licencia, el usuario no puede compartir la Publicación ISO con nadie, ni siquiera en red;

   ii) una licencia de red para el Propósito especificado. La licencia de red puede asignarse a usuarios finales concurrentes sin nombre o a usuarios finales concurrentes con nombre dentro de la misma organización.

b) Propósito:

   i) Propósito interno: uso interno sólo dentro de la organización del usuario, incluyendo, pero no limitado a su propia implementación («Propósito interno»).

   El alcance del uso interno permitido se especifica en el momento de la compra o a través de un acuerdo posterior con ISO, el organismo miembro de ISO en el país del usuario, cualquier otro organismo miembro de ISO o un distribuidor de tercera parte autorizado, incluido cualquier derecho de reproducción interna aplicable (como reuniones internas, programas de formación internos, preparación de servicios de certificación, integración o ilustración en manuales internos, materiales de formación internos y documentos de orientación internos). Cada uso interno debe especificarse explícitamente en la orden de compra, y se aplicarán tarifas y requisitos específicos a cada uso permitido.

   ii) Propósito externo: uso externo, incluyendo pero no limitado a servicios de certificación, consultoría, formación, servicios digitales por parte del usuario/organización del usuario a terceros, así como para fines comerciales y no comerciales («Propósito externo»).

   El alcance del uso externo permitido se especifica en el momento de la compra o a través de un acuerdo posterior con ISO, el organismo miembro de ISO en el país del usuario, cualquier otro organismo miembro de ISO o un distribuidor de tercera parte autorizado, incluyendo cualquier derecho de reproducción externa aplicable (por ejemplo, en publicaciones, productos o servicios comercializados y vendidos por la organización del usuario/usuario). Cada uso externo debe especificarse explícitamente en la orden de compra, y se aplicarán tarifas y requisitos específicos a cada uso permitido.

A menos que a los usuarios se les hayan concedido derechos de reproducción de acuerdo con las disposiciones anteriores, no se les concede el derecho a compartir o sublicenciar las publicaciones de ISO dentro o fuera de su organización para ninguno de los fines. Si los usuarios desean obtener derechos de reproducción adicionales para las publicaciones de ISO o su contenido, los usuarios pueden ponerse en contacto con ISO o con el organismo miembro de ISO en su país para explorar sus opciones.

En caso de que al usuario o a la organización del usuario se le conceda una licencia para el Propósito Externo de proporcionar alguna o todas las actividades en la prestación de servicios de certificación, o para auditar para un cliente, el usuario o la organización del usuario se compromete a verificar que la organización que opera bajo el sistema de gestión sujeto a certificación o auditoría ha obtenido una licencia para su propia implementación de la Norma ISO utilizada para la certificación o auditoría del organismo miembro de ISO en su país, de cualquier otro organismo miembro de ISO, de ISO o de un distribuidor de tercera parte autorizado. Esta obligación de verificación se debe incluir en el acuerdo de licencia aplicable obtenido por el usuario o la organización del usuario.

Las publicaciones de ISO no deben divulgarse a terceros, y los usuarios las deben utilizar únicamente para los fines especificados en la orden de compra y/o en el acuerdo de licencia aplicable. La divulgación no autorizada o el uso de las publicaciones de ISO más allá del Propósito para el que se concedió la licencia están prohibidos y pueden dar lugar a acciones legales.

Restricciones de uso

Salvo lo dispuesto en el Contrato de Licencia aplicable y sujeto a una licencia independiente por parte de ISO, el organismo miembro de ISO en el país del usuario, cualquier otro organismo miembro de ISO o un distribuidor de tercera parte autorizado, no se concede a los usuarios el derecho a:

— utilizar las Publicaciones de ISO para cualquier fin distinto del Propósito;

— conceder derechos de uso o acceso a las Publicaciones de ISO más allá del Tipo de Licencia;

— divulgar las Publicaciones de ISO más allá del Propósito y/o Tipo de Licencia previstos;

— vender, prestar, arrendar, reproducir, distribuir, importar/exportar o explotar comercialmente de cualquier otro modo las Publicaciones de ISO. En el caso de normas conjuntas (como las normas ISO/IEC), esta cláusula se debe aplicar a la respectiva propiedad conjunta de los derechos de autor;

— ceder o transferir de cualquier otro modo la propiedad de las Publicaciones de ISO, en su totalidad o en fragmentos, a terceros.

Independientemente del Tipo de Licencia o Propósito para el que se concedan a los usuarios los derechos de acceso y uso de las publicaciones de ISO, no se permite a los usuarios acceder o utilizar ninguna publicación de ISO, en su totalidad o en fragmentos, para ningún aprendizaje automático y/o inteligencia artificial y/o propósitos similares, incluyendo pero no limitado a acceder o utilizarlos (i) como datos de entrenamiento para grandes modelos de lenguaje o similares, o (ii) para provocar o permitir de otro modo que la inteligencia artificial o herramientas similares generen respuestas. Dicho uso sólo está permitido si está expresamente autorizado mediante un acuerdo de licencia específico por el organismo miembro de ISO en el país del solicitante, otro organismo miembro de ISO o ISO. Las solicitudes de autorización de este tipo pueden estudiarse caso por caso para asegurar el cumplimiento de los derechos de propiedad intelectual.

Si ISO, o el organismo miembro de ISO en el país del usuario, tiene dudas razonables de que los usuarios no cumplen estas condiciones, puede solicitar por escrito la realización de una auditoría, o que un auditor de tercera parte realice una auditoría, durante el horario laboral en las instalaciones del usuario o mediante acceso remoto.

Cualquier comentario o pregunta sobre este documento deberían dirigirse al organismo nacional de normalización del usuario. En www.iso.org/members.html se puede encontrar un listado completo de estos organismos.

Prólogo de la versión en español

Este documento ha sido traducido por el Grupo de Trabajo Spanish Translation Task Force (STTF) del Comité Técnico ISO/TC 309, *Gobernanza de las organizaciones*, en el que participan representantes de los organismos nacionales de normalización y otras partes interesadas, para lograr la unificación de la terminología en lengua española en el ámbito de la gobernanza de las organizaciones.

Este documento ha sido validado por el ISO/TMBG/Spanish Translation Management Group (STMG) conformado por los siguientes países: Argentina, Bolivia, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, España, Guatemala, Honduras, República Dominicana, México, Panamá, Paraguay, Perú y Uruguay.

Introducción

El soborno es un fenómeno generalizado que plantea serias inquietudes sociales, morales, económicas y políticas, socava el buen gobierno, obstaculiza el desarrollo y distorsiona la competencia. Erosiona la justicia, socava los derechos humanos y es un obstáculo para el alivio de la pobreza. También aumenta el costo de hacer negocios, introduce incertidumbres en las transacciones comerciales, aumenta el costo de los bienes y servicios, disminuye la calidad de los productos y servicios, lo que puede conducir a la pérdida de vidas y bienes, destruye la confianza en las instituciones e interfiere con el funcionamiento justo y eficiente de los mercados.

Los gobiernos han avanzado en la lucha contra el soborno mediante acuerdos internacionales como la Convención de la Organización para la Cooperación y el Desarrollo Económicos sobre la lucha contra el soborno de funcionarios públicos extranjeros en las transacciones comerciales internacionales[18] y la Convención de las Naciones Unidas contra la Corrupción[17] y mediante sus leyes nacionales. En la mayoría de las jurisdicciones, constituye un delito que las personas participen en sobornos y existe una tendencia creciente a responsabilizar a las organizaciones, así como a las personas, por soborno.

NOTA a la versión española: En la versión española se han corregido las referencias[18] y[19] a la bibliografía que eran erróneas en la versión inglesa y se han sustituido por[17] y[18] respectivamente.

Sin embargo, la ley por sí sola no es suficiente para resolver este problema. Las organizaciones tienen la responsabilidad de contribuir activamente a combatir el soborno. Esto puede lograrse mediante un sistema de gestión antisoborno, que este documento pretende proporcionar, y mediante el compromiso de liderazgo para establecer una cultura de integridad, transparencia, apertura y cumplimiento. La naturaleza de la cultura de una organización es crítica para el éxito o fracaso de un sistema de gestión antisoborno.

Se espera que una organización bien administrada cuente con una política de *compliance* apoyada por sistemas de gestión adecuados para ayudarla a cumplir sus obligaciones legales y su compromiso con la integridad. Una política contra el soborno es un componente de una política general de *compliance*. La política de lucha contra el soborno y el sistema de gestión que la apoya ayudan a una organización a evitar o mitigar los costos, riesgos y daños de la participación en el soborno, a promover la confianza en los negocios y a mejorar su reputación.

Este documento refleja las buenas prácticas internacionales y puede utilizarse en todas las jurisdicciones. Es aplicable a las organizaciones pequeñas, medianas y grandes de todos los sectores, incluidos los sectores públicos, privado y sin fines de lucro. Los riesgos de soborno que enfrenta una organización varían en función de factores tales como el tamaño de la organización, los lugares y sectores en los que opera la organización, y la naturaleza, escala y complejidad de las actividades de la organización. Este documento especifica la implementación por parte de la organización de políticas, procedimientos y controles que sean razonables y proporcionales de acuerdo con los riesgos de soborno que enfrenta la organización. El Anexo A proporciona orientación sobre la implementación de los requisitos de este documento.

La conformidad con este documento no garantiza que el soborno no haya ocurrido o no vaya a ocurrir en relación con la organización, ya que no es posible eliminar completamente el riesgo de soborno. Sin embargo, este documento puede ayudar a la organización a implementar medidas razonables y proporcionadas diseñadas para prevenir, detectar y responder al soborno.

Este documento puede ser usado en conjunto con otras normas de sistemas de gestión (por ejemplo, ISO 9001, ISO 14001, ISO/IEC 27001, ISO 37301 e ISO 37002) y normas de gestión (por ejemplo, ISO 26000 e ISO 31000).

En la Norma ISO 37000 se especifica la orientación para la gobernanza de las organizaciones y en la Norma ISO 37301 se especifican los requisitos para un sistema general de gestión del *compliance*.

Sistemas de gestión antisoborno — Requisitos con orientación para su uso

1 Objeto y campo de aplicación

Este documento especifica los requisitos y proporciona una orientación para establecer, implementar, mantener, revisar y mejorar un sistema de gestión antisoborno. El sistema puede ser independiente o puede estar integrado en un sistema de gestión global. Este documento aborda lo siguiente en relación con las actividades de la organización:

— soborno en los sectores público, privado y sin fines de lucro;

— soborno por parte de la organización;

— soborno por parte del personal de la organización que actúe en nombre de la organización o para su beneficio;

— soborno de los socios de negocios de la organización que actúen en nombre de la organización o para su beneficio;

— soborno a la organización;

— soborno del personal de la organización en relación con las actividades de la organización;

— soborno de los socios de negocios de la organización en relación con las actividades de la organización;

— soborno directo e indirecto (por ejemplo, un soborno ofrecido o aceptado a través o por un tercero).

Este documento es aplicable solo al soborno. Establece requisitos y proporciona orientación para un sistema de gestión diseñado para ayudar a una organización a prevenir, detectar y enfrentar al soborno y cumplir con las leyes antisoborno y los compromisos voluntarios aplicables a sus actividades.

Los requisitos de este documento son genéricos y se pretende que sean aplicables a todas las organizaciones (o partes de una organización), independientemente del tipo, tamaño y naturaleza de la actividad, ya sea en los sectores público, privado o sin fines de lucro. El grado de aplicación de estos requisitos depende de los factores especificados en los apartados 4.1, 4.2 y 4.5.

NOTA 1 Véase el Capítulo A.2 para orientación.

NOTA 2 Las medidas necesarias para prevenir, detectar y mitigar el riesgo de soborno por parte de la organización pueden ser diferentes de las medidas utilizadas para prevenir, detectar y responder al soborno de la organización (o de su personal o socios de negocios que actúan en nombre de la organización). Véase el Capítulo A.8 para orientación.

2 Referencias normativas

No existen referencias normativas en este documento.

3 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones siguientes:

ISO e IEC mantienen bases de datos terminológicas para su utilización en normalización en las siguientes direcciones:

— Plataforma de búsqueda en línea de ISO: disponible en https://www.iso.org/obp

— Electropedia de IEC: disponible en https://www.electropedia.org/

3.1
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* (3.16) de las obligaciones de esa persona

Nota 1 a la entrada: Lo anterior es una definición genérica. El significado del término "soborno" es el definido por las leyes antisoborno aplicables a la *organización* (3.2) y por el *sistema de gestión* (3.5) antisoborno diseñado por la organización.

3.2
organización
persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus *objetivos* (3.11)

Nota 1 a la entrada: El concepto de organización incluye, entre otros, un trabajador independiente, compañía, corporación, firma, empresa, autoridad, sociedad, organización benéfica o institución, o una parte o combinación de estas, ya estén constituidas o no, públicas o privadas.

Nota 2 a la entrada: Si la organización forma parte de una entidad más grande, el término «organización» se refiere únicamente a la parte de la entidad más grande que está dentro del alcance del *sistema de gestión* (3.5) antisoborno.

3.3
parte interesada
persona u *organización* (3.2) que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad

Nota 1 a la entrada: Una parte interesada puede ser interna o externa a la organización.

3.4
requisito
necesidad que está establecida y es obligatoria

Nota 1 a la entrada: La definición esencial de "requisito" en normas ISO de sistemas de gestión es "necesidad o expectativa establecida, generalmente implícita u obligatoria". La parte de los "requisitos generalmente implícitos" no es aplicable en el contexto de gestión antisoborno.

Nota 2 a la entrada: "Generalmente implícita" significa que es habitual o práctica común para la *organización* (3.2) y las *partes interesadas* (3.3) el que la necesidad o expectativa bajo consideración está implícita.

Nota 3 a la entrada: Un requisito específico es aquel que es establecido, por ejemplo, en la *información documentada* (3.14).

3.5
sistema de gestión
conjunto de elementos de una *organización* (3.2) interrelacionados o que interactúan para establecer *políticas* (3.10), *objetivos* (3.11), así como *procesos* (3.15) para lograr estos objetivos

Nota 1 a la entrada: Un sistema de gestión puede considerar una sola disciplina o varias disciplinas.

Nota 2 a la entrada: Los elementos del sistema de gestión incluyen la estructura, los roles y las responsabilidades, la planificación y la operación de la organización.

Nota 3 a la entrada: El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones.

3.6
alta dirección
persona o grupo de personas que dirigen y controlan una *organización* (3.2) al más alto nivel

Nota 1 a la entrada: La alta dirección tiene el poder para delegar autoridad y proporcionar recursos dentro de la organización.

Nota 2 a la entrada: Si el alcance del sistema de *gestión* (3.5) comprende solo una parte de la organización, entonces la alta dirección se refiere a quienes dirigen y controlan esa parte de la organización.

Nota 3 a la entrada: Las organizaciones pueden organizarse dependiendo del marco legal bajo el cual están obligadas a operar y también de acuerdo a su tamaño, sector, etc. Algunas organizaciones poseen tanto un *órgano de gobierno* (3.7) como *alta dirección* (3.6), mientras que algunas organizaciones no tienen divididas las responsabilidades en varios órganos. Estas variaciones, tanto en lo que se refiere a la organización como a las responsabilidades, pueden ser consideradas cuando se aplican los requisitos en el Capítulo 5.

3.7
órgano de gobierno
persona o grupo de personas que tienen la rendición de cuentas final de toda la *organización* (3.2)

Nota 1 a la entrada: Un órgano de gobierno puede establecerse explícitamente en varios formatos, que incluyen, entre otros, directorio, consejo directivo, directores individuales, directorio como conjunto o individualmente o directivos o administradores.

Nota 2 a la entrada: Las normas de sistemas de gestión ISO hacen referencia al término “alta dirección” para describir un rol que, según la norma y el contexto organizacional, reporta o es responsable ante el órgano de gobierno.

Nota 3 a la entrada: No todas las organizaciones, en particular las pequeñas y medianas, tendrán un órgano de gobierno separado de la alta dirección. En tales casos, la alta dirección ejerce el rol de órgano de gobierno.

[FUENTE: ISO 37000:2021, 3.3.4, modificado — Las Notas a la entrada fueron reordenadas: La Nota 2 a la entrada ahora es Nota 1 a la entrada; la Nota 3 a la entrada ahora es Nota 2 a la entrada; y se agregó la Nota 3 a la entrada.]

3.8
función antisoborno
personas con responsabilidad y autoridad para la operación del *sistema de gestión* (3.5) antisoborno

3.9
eficacia
grado en el cual se realizan las actividades planificadas y se logran los resultados planificados

3.10
política
intenciones y dirección de una *organización* (3.2), como las expresa formalmente su *alta dirección* (3.6) o su *órgano de gobierno* (3.7)

3.11
objetivo
resultado a lograr

Nota 1 a la entrada: Un objetivo puede ser estratégico, táctico u operacional.

Nota 2 a la entrada: Los objetivos pueden referirse a diferentes disciplinas (tales como objetivos financieros, ventas y marketing, compras, de salud y seguridad y ambientales), y se pueden aplicar en diferentes niveles como estratégicos, para toda la organización, para el proyecto, el producto y el *proceso* (3.15).

Nota 3 a la entrada: Un objetivo se puede expresar de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operacional, un objetivo antisoborno, o mediante el uso de términos con un significado similar (por ejemplo, fin o meta).

Nota 4 a la entrada: En el contexto de *sistemas de gestión* (3.5) antisoborno, la *organización* (3.2) establece los objetivos antisoborno, de forma coherente con la *política* (3.10) antisoborno, para lograr resultados específicos.

3.12
riesgo
efecto de la incertidumbre

Nota 1 a la entrada: Un efecto es una desviación de lo esperado, ya sea positivo o negativo.

Nota 2 a la entrada: Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o su posibilidad.

Nota 3 a la entrada: Con frecuencia el riesgo se caracteriza por referenciar a eventos potenciales y consecuencias, o a una combinación de estos.

Nota 4 a la entrada: Con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos cambios en las circunstancias) y la probabilidad asociada de que ocurra.

3.13
competencia
capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos

3.14
información documentada
información que una *organización* (3.2) tiene que controlar y mantener, y el medio de soporte que la contiene

Nota 1 a la entrada: La información documentada puede estar en cualquier formato y medio de soporte, y puede provenir de cualquier fuente.

Nota 2 a la entrada: La información documentada puede hacer referencia a:

— el sistema *de gestión* (3.5), incluidos los *procesos* (3.15) relacionados;

— la información generada para que la organización opere (documentación);

— la evidencia de los resultados alcanzados (registros).

3.15
proceso
conjunto de actividades interrelacionadas o que interactúan, que usa o transforma las entradas para producir un resultado

Nota 1 a la entrada: El hecho de que el resultado de un proceso se denomine una salida, un producto o un servicio depende del contexto de referencia.

3.16
desempeño
resultado medible

Nota 1 a la entrada: El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

Nota 2 a la entrada: El desempeño se puede relacionar con la gestión de actividades, *procesos* (3.15), productos, servicios, sistemas u *organizaciones* (3.2).

3.17
seguimiento
determinación del estado de un sistema, un *proceso* (3.15) o una actividad

Nota 1 a la entrada: Para determinar el estado puede ser necesario verificar, supervisar u observar en forma crítica.

3.18
medición
proceso (3.15) para determinar un valor

3.19
auditoría
proceso (3.15) sistemático e independiente para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría

Nota 1 a la entrada: Una auditoría puede ser interna (de primera parte), o externa (de segunda parte o de tercera parte), y puede ser combinada (combinando dos o más disciplinas).

Nota 2 a la entrada: Una auditoría interna la realiza la propia *organización* (3.2) o una parte externa que actúe en su nombre.

Nota 3 a la entrada: "Evidencia de auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011.

3.20
conformidad
cumplimiento de un *requisito* (3.4)

3.21
no conformidad
incumplimiento de un *requisito* (3.4)

3.22
acción correctiva
acción para eliminar las causas de una *no conformidad* (3.21) y prevenir que vuelvan a ocurrir

3.23
mejora continua
actividad recurrente para mejorar el *desempeño* (3.16)

3.24
personal
directores, funcionarios, empleados, empleados o trabajadores temporales y voluntarios de la *organización* (3.2)

Nota 1 a la entrada: Diferentes tipos de personal plantean diferentes tipos y grados de *riesgo* (3.12) de soborno y, por lo tanto, pueden tratarse de manera diferente por los procedimientos de evaluación de riesgo de soborno y de gestión de riesgos de soborno de la organización.

Nota 2 a la entrada: Véase el Capítulo A.8 para orientación sobre los empleados o trabajadores temporales.

3.25
socio de negocios
parte externa con la que la *organización* (3.2) tiene, o planifica establecer, algún tipo de relación comercial

Nota 1 a la entrada: Socio de negocios incluye pero no se limita a los clientes, consumidores, "alianza empresarial", socios de alianzas empresariales, miembros de un consorcio, proveedores externos, contratistas, consultores, subcontratistas, proveedores, vendedores, asesores, agentes, distribuidores, representantes, intermediarios e inversores. Esta definición es deliberadamente amplia y debería interpretarse de acuerdo con el perfil de *riesgo* (3.12) de soborno de la organización, para que se aplique a los socios de negocios que razonablemente se entienda que pueden exponer a la organización a riesgos de soborno.

Nota 2 a la entrada: Diferentes tipos de socio de negocios plantean diferentes tipos y grados de riesgo de soborno, y una *organización* (3.2) tendrá diferentes grados de capacidad para influir en diferentes tipos de socio de negocios. Por lo tanto, diferentes tipos de socio de negocios pueden tratarse de manera diferente por los procedimientos de evaluación de riesgo de soborno y de gestión de riesgos de soborno de la organización.

Nota 3 a la entrada: La referencia a "negocio" en este documento puede interpretarse en sentido amplio para significar aquellas actividades que son relevantes a los efectos de la existencia de la organización.

3.26
funcionario público
toda persona que ocupe un cargo legislativo, administrativo o judicial, por designación, elección o como sucesor, o cualquier persona que ejerza una función pública, incluso para un organismo público o una empresa pública, o cualquier funcionario o agente de una organización pública local o internacional, o cualquier candidato a un cargo público

Nota 1 a la entrada: Para ejemplos de personas que pueden considerarse como funcionarios públicos, véase el Capítulo A.21.

3.27
tercera parte
persona u organismo que es independiente de la *organización* (3.2)

Nota 1 a la entrada: Todos los *socios de negocios* (3.25) son tercera parte, pero no todas las terceras partes son socios de negocios.

3.28
conflicto de interés
situación en la que una parte interesada tiene un interés personal o un interés organizacional, directa o indirectamente, que puede comprometer o interferir en la capacidad de actuar imparcialmente en el desempeño de sus funciones en el mejor interés de la organización

Nota 1 a la entrada: Puede haber diferentes tipos de intereses personales: comerciales, financieros, familiares, profesionales, religiosos o políticos.

Nota 2 a la entrada: El interés organizacional se relaciona con los intereses de una organización o parte de una organización (por ejemplo, equipo o departamento) en lugar de los de un individuo.

[FUENTE: ISO 37009:—[1)], 3.14]

3.29
debida diligencia
proceso (3.15) para evaluar con mayor detalle la naturaleza y alcance del *riesgo* (3.12) de soborno y para ayudar a las *organizaciones* (3.2) a tomar decisiones en relación con transacciones, proyectos, actividades, *socios de negocios* (3.25) y *personal* (3.24) específicos

3.30
cultura antisoborno
valores, ética, creencias y conductas que existen en una *organización* (3.2) y que interactúan con las estructuras y sistemas de control de la organización para producir normas de comportamiento que conducen a la *política* (3.10) antisoborno y al sistema de gestión (3.5) antisoborno

Nota 1 a la entrada: Este término ha sido adaptado de la Norma ISO 37301:2021, 3.28, “cultura de *compliance*”.

4 Contexto de la organización

4.1 Comprensión de la organización y de su contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos en su sistema de gestión antisoborno. Estas cuestiones incluyen, pero sin limitarse, a los siguientes factores:

a) el tamaño, la estructura y la delegación de autoridad con poder de decisión de la organización;

b) los lugares y sectores en los que opera la organización o anticipa operar;

c) la naturaleza, escala y complejidad de las actividades y operaciones de la organización;

1) En desarrollo. Etapa en el momento de publicación: ISO/DIS 37009:2025.

d) el modelo de negocio de la organización;

e) las entidades sobre las que la organización tiene el control y entidades que ejercen control sobre la organización;

f) los socios de negocios de la organización;

g) la naturaleza y el alcance de las interacciones con los funcionarios públicos;

h) los deberes y obligaciones legales, reglamentarios, contractuales y profesionales aplicables.

La organización debe determinar si el cambio climático es una cuestión pertinente.

NOTA Una organización tiene control sobre otra organización si controla directa o indirectamente la gestión de esa organización (véase A.13).

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas que son pertinentes para el sistema de gestión antisoborno;

b) los requisitos pertinentes de estas partes interesadas;

c) cuáles de esos requisitos se abordarán mediante el sistema de gestión antisoborno.

NOTA 1 Las partes interesadas pertinentes pueden tener requisitos relacionados con el cambio climático.

NOTA 2 En la identificación de los requisitos de las partes interesadas, una organización puede distinguir entre los requisitos obligatorios y las expectativas de carácter no obligatorio de las partes interesadas, así como los compromisos voluntarios asumidos con ellas.

4.3 Determinación del alcance del sistema de gestión antisoborno

La organización debe determinar los límites y la aplicabilidad del sistema de gestión antisoborno para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:

a) las cuestiones externas e internas indicadas en el apartado 4.1;

b) los requisitos indicados en el apartado 4.2;

c) los resultados de la evaluación del riesgo de soborno referida en el apartado 4.5.

El alcance debe estar disponible como información documentada.

NOTA Véase el Capítulo A.2 para orientación.

4.4 Sistema de gestión antisoborno

La organización debe establecer, implementar, mantener y mejorar continuamente el sistema de gestión antisoborno, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

El sistema de gestión antisoborno debe estar documentado y debe contener medidas diseñadas para identificar y evaluar el riesgo de soborno, y para prevenir, detectar y enfrentar el riesgo de soborno.

NOTA 1 No es posible eliminar por completo el riesgo de soborno y ningún sistema de gestión antisoborno será capaz de prevenir y detectar todos los sobornos.

El sistema de gestión antisoborno debe ser razonable y proporcionado, teniendo en cuenta los factores mencionados en el apartado 4.3.

NOTA 2 Véase el Capítulo A.3 para orientación.

4.5 Evaluación del riesgo de soborno

4.5.1 La organización debe realizar a intervalos planificados evaluaciones del riesgo de soborno que deben:

a) identificar los riesgos de soborno que la organización puede anticipar razonablemente teniendo en cuenta los factores enumerados en el apartado 4.1;

b) analizar, evaluar y priorizar los riesgos de soborno identificados;

c) evaluar la idoneidad y eficacia de los controles existentes de la organización para mitigar los riesgos de soborno evaluados.

4.5.2 La organización debe establecer criterios para evaluar su nivel de riesgo de soborno, que debe tener en cuenta las políticas y objetivos de la organización.

4.5.3 La evaluación del riesgo de soborno debe ser revisada:

a) a intervalos planificados de modo que los cambios y la nueva información puedan evaluarse adecuadamente, con base en el tiempo y la frecuencia definidos por la organización;

b) en el caso de un cambio significativo en la estructura o las actividades de la organización.

4.5.4 La organización debe conservar la información documentada que demuestra que se ha llevado a cabo la evaluación del riesgo de soborno, y que se ha utilizado para diseñar o mejorar continuamente el sistema de gestión antisoborno.

NOTA Véase el Capítulo A.4 para orientación.

5 Liderazgo

5.1 Liderazgo y compromiso

5.1.1 Órgano de gobierno

Cuando la organización cuente con un órgano de gobierno separado, dicho órgano debe demostrar su liderazgo y compromiso con respecto al sistema de gestión antisoborno:

a) aprobando la política antisoborno de la organización;

b) asegurando que la estrategia de la organización y la política antisoborno se encuentren alineadas;

c) recibiendo y revisando, a intervalos planificados, la información sobre el contenido y el funcionamiento del sistema de gestión antisoborno de la organización;

d) requiriendo que los recursos adecuados y apropiados, necesarios para el funcionamiento eficaz del sistema de gestión antisoborno, sean asignados y distribuidos;

e) ejerciendo una supervisión razonable sobre la implementación del sistema de gestión antisoborno de la organización por la alta dirección, sus resultados esperados y su eficacia.

Estas actividades deben llevarse a cabo por la alta dirección, si la organización no tiene un órgano de gobierno separado.

Para obtener más orientación sobre los roles del órgano de gobierno y la alta dirección, véase la Norma ISO 37000:2021, 4.2.3.

5.1.2 Alta dirección

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión antisoborno:

a) asegurando que se establezcan la política antisoborno y los objetivos antisoborno;

b) asegurando la integración de los requisitos del sistema de gestión antisoborno en los procesos de negocio de la organización;

c) asegurando que los recursos necesarios para el sistema de gestión antisoborno estén disponibles;

d) comunicando interna y externamente lo relacionado con la política antisoborno;

e) comunicando la importancia de una gestión antisoborno eficaz y de cumplir con los requisitos del sistema de gestión antisoborno;

f) asegurando que el sistema de gestión antisoborno logre los resultados previstos;

g) dirigiendo y apoyando al personal para que contribuya a la eficacia del sistema de gestión antisoborno;

h) promoviendo una cultura antisoborno apropiada dentro de la organización;

i) promoviendo la mejora continua;

j) apoyando a otros roles pertinentes, para demostrar su liderazgo en la prevención y detección de soborno en la medida en la que se aplique a sus áreas de responsabilidad;

k) fomentando el uso de los procedimientos de denuncia para plantear inquietudes sobre sospecha de soborno y el soborno real (véase 8.9);

l) asegurando que ningún miembro del personal sufrirá represalias, discriminación o medidas disciplinarias (excepto cuando el individuo participó en la violación) [véase 7.2.2.1 d)] por informes hechos de buena fe o sobre la base de una creencia razonable de violación o sospecha de violación de la política antisoborno o del sistema de gestión antisoborno de la organización, o por negarse a participar en el soborno, incluso si tal negativa puede dar lugar a la pérdida de negocios para la organización;

m) informando a intervalos planificados, al órgano de gobierno sobre el contenido y el funcionamiento del sistema de gestión antisoborno y de las denuncias de soborno graves y/o sistemáticas.

NOTA 1 En este documento se puede interpretar el término “negocio” en su sentido más amplio para referirse a aquellas actividades que son pertinentes para el fin de la existencia de la organización.

NOTA 2 Véase el Capítulo A.5 para orientación.

5.1.3 Cultura antisoborno

La organización debe desarrollar, mantener y promover una cultura antisoborno en todos los niveles de la organización.

El órgano de gobierno, la alta dirección y la dirección deben demostrar un compromiso activo, visible, coherente y sostenido hacia un estándar común de comportamiento y conducta que se requiere en toda la organización.

La alta dirección debe fomentar un comportamiento que apoye la política antisoborno y el sistema de gestión antisoborno. Debe prevenir y no tolerar comportamientos que comprometan la lucha contra el soborno.

NOTA Véase el Capítulo A.5 para orientación.

5.2 Política antisoborno

La alta dirección debe establecer una política antisoborno que:

a) prohíba el soborno;

b) requiera del cumplimiento de las leyes antisoborno que sean aplicables a la organización;

c) sea apropiada al propósito de la organización;

d) proporcione un marco de referencia para el establecimiento de los objetivos antisoborno;

e) incluya el compromiso de cumplir los requisitos aplicables;

f) promueva el planteamiento de inquietudes de buena fe o sobre la base de una creencia razonable, en confianza y sin temor a represalias;

g) incluya un compromiso de mejora continua del sistema de gestión antisoborno;

h) explique la autoridad y la independencia de la función antisoborno;

i) explique las consecuencias de no cumplir con la política antisoborno.

La política antisoborno debe:

— estar disponible como información documentada;

— comunicarse dentro de la organización;

— estar disponible para las partes interesadas, según corresponda;

— comunicarse a los socios de negocios que representen más que un riesgo bajo de soborno.

5.3 Roles, responsabilidades y autoridades

5.3.1 Generalidades

La alta dirección debe tener la responsabilidad general de la implementación y el *compliance* del sistema de gestión antisoborno.

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen y comuniquen dentro de la organización.

Los gerentes en cada nivel deben ser responsables de requerir que el sistema de gestión antisoborno se aplique y se cumpla en su departamento o función.

El órgano de gobierno, la alta dirección y cualquier otro miembro del personal deben ser responsables de entender, cumplir y aplicar el sistema de gestión antisoborno en lo que respecta a su rol en la organización.

5.3.2 Función antisoborno

La función antisoborno debe tener la responsabilidad y autoridad para:

a) asegurar que el sistema de gestión antisoborno cumple con los requisitos de este documento;

b) informar sobre el desempeño del sistema de gestión antisoborno al órgano de gobierno y a la alta dirección;

c) supervisar el diseño y la implementación del sistema de gestión antisoborno por parte de la organización;

d) proporcionar asesoramiento y orientación al personal y a las partes interesadas sobre el sistema de gestión antisoborno y los asuntos relacionados con el soborno.

Se debe proveer de recursos adecuados a la función antisoborno y asignarla a las personas que tengan la competencia, el estatus, la autoridad y la independencia apropiadas.

La función antisoborno debe tener acceso directo y rápido al órgano de gobierno y a la alta dirección en el caso de que necesite plantear cualquier asunto o inquietud en relación con el soborno o el sistema de gestión antisoborno.

NOTA Véase el Capítulo A.6 para orientación.

La alta dirección puede asignar parte o la totalidad de la función antisoborno a personas externas a la organización. Si lo hace, la alta dirección debe asegurar que personal específico tenga la responsabilidad y autoridad sobre aquellas partes de la función asignadas externamente.

5.3.3 Delegación de la toma de decisiones

Cuando la alta dirección delegue al personal la autoridad para la toma de decisiones en las que existe más que un riesgo bajo de soborno, la organización debe establecer y mantener un proceso de toma de decisiones o un conjunto de controles que requieran que el proceso de toma de decisiones y el nivel de autoridad de las personas que toman las decisiones sean apropiados y estén libres de conflictos de interés reales o potenciales. La alta dirección debe asegurarse de que estos procesos se revisen a intervalos planificados como parte de sus roles y responsabilidades para la implementación y el cumplimiento del sistema de gestión antisoborno que se describe en el apartado 5.3.1.

NOTA La delegación de toma de decisiones no exime a la alta dirección o al órgano de gobierno, de sus deberes y responsabilidades descritas en los apartados 5.1.1, 5.1.2 y 5.3.1, ni transfiere, necesariamente, las potenciales responsabilidades legales al que se le delegó esta función.

6 Planificación

6.1 Acciones para abordar los riesgos y oportunidades

Al planificar el sistema de gestión antisoborno, la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario abordar con el fin de:

a) asegurar que el sistema de gestión antisoborno pueda lograr sus resultados previstos;

b) prevenir o reducir efectos no deseados;

c) lograr la mejora continua;

d) hacer seguimiento de la eficacia del sistema de gestión antisoborno;

La organización debe planificar:

i) las acciones para abordar estos riesgos y oportunidades;

ii) la manera de:

- integrar e implementar estas acciones en sus procesos del sistema de gestión antisoborno;
- evaluar la eficacia de estas acciones.

6.2 Objetivos antisoborno y planificación para lograrlos

La organización debe establecer los objetivos antisoborno para las funciones y niveles pertinentes.

Los objetivos antisoborno deben:

a) ser coherentes con la política antisoborno;

b) ser medibles (si es posible);

c) tener en cuenta los requisitos aplicables;

d) ser objeto de seguimiento;

e) comunicarse;

f) actualizarse, según corresponda;

g) estar disponibles como información documentada;

h) ser alcanzables.

Al planificar cómo lograr sus objetivos antisoborno, la organización debe determinar:

— qué se va a hacer;

— qué recursos se requerirán;

— quién será responsable;

— cuándo se alcanzarán los objetivos;

— cómo se evaluarán los resultados;

— quién impondrá sanciones o penalizaciones.

6.3 Planificación de cambios

Cuando la organización determine la necesidad de ~~realizar~~ cambios en el sistema de gestión antisoborno, los cambios deben llevarse a cabo de manera planificada.

NOTA Véase el Capítulo A.20 para orientación.

7 Apoyo

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión antisoborno.

NOTA Véase el Capítulo A.7 para orientación.

7.2 Competencia

7.2.1 Generalidades

La organización debe:

a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en relación con el antisoborno;

b) asegurarse que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas;

c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas;

Debe estar disponible la información documentada apropiada como evidencia de la competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

7.2.2 Proceso de contratación

7.2.2.1 En relación con todo su personal, la organización debe implementar procedimientos de manera que:

a) las condiciones de empleo requieran que el personal cumpla con la política antisoborno y el sistema de gestión antisoborno y den a la organización el derecho para disciplinar al personal en caso de incumplimiento;

b) en un período razonable desde el inicio de su relación laboral, el personal reciba una copia de la política antisoborno, o se le proporcione acceso a ella y a la formación en relación con esta política;

c) la organización disponga de procedimientos que le permitan tomar medidas disciplinarias apropiadas contra el personal que viole la política antisoborno o el sistema de gestión antisoborno; y

d) el personal no sufra represalias, discriminación o medidas disciplinarias (por ejemplo, mediante amenazas, aislamiento, degradación, impedimentos para su ascenso, traslado, despido, bullying, victimización u otras formas de acoso) por:

   1) negarse a participar en, o por rechazar, cualquier actividad respecto de la cual ellos hayan juzgado razonablemente que exista más que un riesgo bajo de soborno que no haya sido mitigado por la organización; o

   2) las inquietudes planteadas o informes hechos de buena fe o sobre la base de una creencia razonable, de intento real o sospecha de soborno o violaciones de la política antisoborno o del sistema de gestión antisoborno (excepto cuando el individuo participó en la violación).

e) el personal tome conciencia sobre la necesidad de informar sobre los conflictos de interés potenciales y reales.

NOTA Véase el Capítulo A.8 para orientación.

7.2.2.2 En relación con todas las posiciones que están expuestas a más que un riesgo bajo de soborno, según lo determinado en la evaluación del riesgo de soborno (véase 4.5), y con la función antisoborno, la organización debe implementar procedimientos que proporcionen que:

a) la debida diligencia (véase 8.2) se lleve a cabo sobre las personas antes de que sean empleadas, y sobre el personal antes de que sea transferido o promovido por la organización, para determinar, en la medida de lo razonable, que es apropiado emplearlos o reubicarlos y que es razonable creer que van a cumplir con los requisitos de la política antisoborno y del sistema de gestión antisoborno;

b) los bonos de desempeño, las metas de desempeño y otros elementos de remuneración incentivadores se revisen a intervalos planificados para comprobar que hay garantías razonables en marcha para evitar que fomenten el soborno;

c) dicho personal, la alta dirección y el órgano de gobierno, presenten una declaración, a intervalos planificados, proporcional al riesgo de soborno identificado, confirmando su cumplimiento con la política antisoborno y el sistema de gestión antisoborno.

NOTA 1 La declaración de cumplimiento antisoborno puede ser independiente o formar un componente de un proceso de declaración de cumplimiento más amplio.

NOTA 2 Véase el Capítulo A.8 para orientación.

7.3 Toma de conciencia

7.3.1 Toma de conciencia del personal

El personal debe tomar conciencia de:

a) la política antisoborno, los procedimientos y el sistema de gestión antisoborno de la organización y su deber de cumplir con ellos;

b) su contribución a la eficacia del sistema de gestión antisoborno, incluidos los beneficios de una mejora del desempeño en relación con el antisoborno y de informar cualquier sospecha de soborno;

c) las implicaciones de no cumplir los requisitos del sistema de gestión antisoborno;

d) los procedimientos y el sistema de gestión antisoborno de la organización y su deber de cumplir con ellos;

e) los beneficios de informar sospechas de soborno;

f) cómo y a quién deben informar de cualquier inquietud (véase 8.9).

La organización debe conservar información documentada sobre el programa de toma de conciencia y cuándo y a quién se proporcionó.

7.3.2 Formación del personal

La organización debe proporcionar al personal una formación relacionada con el antisoborno adecuada y apropiada. Dicha formación debe abordar los siguientes asuntos, según corresponda, teniendo en cuenta los resultados de la evaluación del riesgo de soborno (véase 4.5):

a) las políticas y los procedimientos aplicables;

b) el riesgo de soborno y el daño que puede ocasionarles al personal y a la organización como resultado del soborno;

c) las circunstancias en las que puede producirse soborno en relación con sus funciones, y cómo reconocer estas circunstancias;

d) cómo reconocer y responder a las solicitudes u ofertas de sobornos;

e) cómo pueden ayudar a prevenir y evitar el soborno y reconocer los indicadores clave de riesgo de soborno;

f) información sobre la formación y los recursos disponibles.

La organización debe conservar información documentada sobre los procedimientos de formación, el contenido de la formación y cuándo y a quién se proporcionó.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

7.3.3 Formación para socios de negocios

Teniendo en cuenta los riesgos de soborno identificados (véase 4.5), la organización también debe implementar procedimientos que aborden la formación relacionada con el antisoborno para los socios de negocios que actúen en su nombre o en su beneficio, y que puedan representar más que un riesgo bajo de soborno para la organización. Estos procedimientos deben identificar a los socios de negocios para los que es necesaria dicha formación, su contenido y los medios por los cuales se la debe proporcionar.

En el caso de los socios de negocios para los que sea necesaria dicha formación, la organización debe conservar información documentada sobre los procedimientos de formación, el contenido de la formación y cuándo y a quién se proporcionó.

NOTA Los requisitos de formación para los socios de negocios pueden comunicarse a través de requisitos contractuales o similares, y pueden ser implementados por la organización, el socio de negocios o por otras partes designadas para ese propósito.

7.3.4 Programas de toma de conciencia y formación

Se debe proporcionar al personal actividades de toma de conciencia y formación relacionada con el antisoborno desde el momento en que comience a trabajar y a intervalos planificados determinados por la organización, según corresponda a sus roles, los riesgos de soborno a los que esté expuesto y cualquier cambio en las circunstancias. Los programas de toma de conciencia y formación se deben actualizar a intervalos planificados, según sea necesario, para reflejar la nueva información pertinente.

NOTA Véase el Capítulo A.9 para orientación.

7.4 Comunicación

7.4.1 La organización debe determinar las comunicaciones internas y externas pertinentes al sistema de gestión antisoborno, incluyendo:

a) qué comunicar;

b) cuándo comunicar;

c) a quién comunicar;

d) cómo comunicar;

e) quién comunica;

f) en qué idiomas comunicar.

7.4.2 La política antisoborno se debe poner a disposición de todo el personal de la organización y socios de negocios, en los idiomas apropiados, se debe comunicar directamente tanto al personal como a los socios de negocios que representen más que un riesgo bajo de soborno, y se debe publicar a través de canales de comunicación internos y externos de la organización, según sea apropiado.

7.5 Información documentada

7.5.1 Generalidades

El sistema de gestión antisoborno de la organización debe incluir:

a) la información documentada requerida por este documento;

b) la información documentada que la organización determina como necesaria para la eficacia del sistema de gestión antisoborno.

NOTA 1 La extensión de la información documentada para un sistema de gestión antisoborno puede variar de una organización a otra, debido a:

— el tamaño de la organización y su tipo de actividades, procesos, productos y servicios;

— la complejidad de los procesos y sus interacciones;

— la competencia del personal.

NOTA 2 La información documentada puede conservarse por separado como parte del sistema de gestión antisoborno, o puede conservarse como parte de otros sistemas de gestión (por ejemplo, de *compliance*, financiero, comercial, de auditoría).

NOTA 3 Véase el Capítulo A.17 para orientación.

7.5.2 Creación y actualización de la información documentada

Al crear y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);

c) la revisión y aprobación con respecto a la idoneidad y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión antisoborno y por este documento se debe controlar para asegurarse de que:

a) esté disponible y sea adecuada para su uso, donde y cuando se necesite;

b) esté protegida adecuadamente (por ejemplo, contra pérdida de confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

— distribución, acceso, recuperación y ~~el~~ uso;

— almacenamiento y ~~la~~ preservación, incluida la preservación de la legibilidad;

— control de cambios (por ejemplo, control de versión);

— retención y disposición.

La información documentada de origen externo que la organización determina como necesaria para la planificación y operación del sistema de gestión antisoborno se debe identificar, según sea apropiado, y controlar.

NOTA El acceso puede implicar una decisión con relación al permiso solamente para consultar la información documentada, o al permiso y a la autoridad para consultar y modificar la información documentada.

8 Operación

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas en el Capítulo 6, mediante:

a) el establecimiento de criterios para los procesos;

b) la implementación del control de los procesos de acuerdo con los criterios.

Debe estar disponible la información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.

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.

La organización debe asegurarse de que se controlen los procesos, productos o servicios suministrados externamente que son pertinentes para el sistema de gestión antisoborno.

Estos procesos deben incluir los controles específicos mencionados en los apartados 8.2 a 8.10.

NOTA Una organización externa está fuera del alcance del sistema de gestión, aunque la función o el proceso proporcionado externamente esté dentro del alcance.

8.2 Debida diligencia

Cuando la evaluación del riesgo de soborno de la organización ha evaluado más que un riesgo bajo de soborno en relación con:

a) categorías específicas de transacciones, proyectos o actividades,

b) relaciones existentes o planificadas con categorías específicas 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 puedan tenerse en cuenta debidamente.

NOTA 1 La organización puede concluir que es innecesario, injustificado o desproporcionado el llevar a cabo la debida diligencia en ciertas categorías del personal y socios de negocios.

NOTA 2 Los factores enumerados en a), b) y c) anteriores no son exhaustivos.

NOTA 3 Véase el Capítulo A.10 para orientación.

8.3 Controles financieros

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

NOTA Véase el Capítulo A.11 para orientación.

8.4 Controles no financieros

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

NOTA 1 Cualquier transacción particular, actividad o relación puede ser objeto de controles tanto financieros como no financieros.

NOTA 2 Véase el Capítulo A.12 para orientación.

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:

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.

NOTA Una organización tiene control sobre otra organización si controla directa o indirectamente la gestión de la organización (véase A.13).

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 pertinente, la organización debe implementar procedimientos de la siguiente manera:

a) la organización debe determinar si el socio de negocios tiene implementados controles antisoborno que gestionen el riesgo pertinente de soborno;

b) donde un socio de negocios no tenga en marcha controles antisoborno, o no sea 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 pertinente, o

   2) donde no sea 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 negocios (véase 4.5 y 8.2), y la forma en que la organización gestiona dichos riesgos (véase 8.3, 8.4 y 8.5).

NOTA Véase el Capítulo A.13 para orientación.

8.6 Compromisos antisoborno

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 pertinente;

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 pertinente.

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 (véase 4.5 y 8.2), y la forma en que la organización gestiona dichos riesgos (véase 8.3, 8.4 y 8.5).

NOTA Véase el Capítulo A.14 para orientación.

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.

NOTA Véase el Capítulo A.15 para orientación.

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 otras 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 informen, 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 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 de represalias a los que realicen el informe, después de que ellos, de buena fe o sobre la base de una creencia razonable, hayan planteado o informado una inquietud sobre intentos de soborno, supuestos o reales o violaciones a la política antisoborno o el 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 tome conciencia de los procedimientos de informe, y que sean capaces de utilizarlos, y tomen conciencia de sus derechos y protecciones de conformidad con los procedimientos.

NOTA 1 Estos procedimientos pueden ser los mismos, o formar parte de los que se utilizan para el informe de otros asuntos que puedan generar preocupación (por ejemplo, seguridad, negligencia, irregularidad o de otro riesgo grave).

NOTA 2 La organización puede usar un socio de negocios para gestionar el sistema de reporte en su nombre.

NOTA 3 En algunas jurisdicciones, los requisitos en b) y c) anteriores están prohibidos por la ley. En estos casos, la organización documenta que no los puede cumplir.

NOTA 4 Para mayor orientación, véase la Norma ISO 37002.

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 violación de la política antisoborno o el sistema de gestión antisoborno, que haya sido informado, detectado o se sospeche razonablemente;

b) requerir medidas apropiadas en caso de que la investigación revele algún soborno o violación 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 estatus y los resultados de la investigación se informen a la función antisoborno y a otras funciones de *compliance*, según corresponda;

f) requerir que la investigación se lleve a cabo de forma confidencial y que sus productos sean confidenciales.

La investigación debe ser realizada por, e informada a, el personal que no forme parte del rol o función que se esté investigando. La organización puede nombrar a un socio de negocios para llevar a cabo la investigación e informar de los resultados a los miembros del personal que no formen parte del rol o función que se esté investigando.

NOTA 1 Véase el Capítulo A.18 para orientación.

NOTA 2 En algunas jurisdicciones, el requisito en f) está prohibido por la ley. En estos casos, la organización documenta que no lo puede cumplir.

NOTA 3 Para mayor orientación, véase la Especificación Técnica ISO/TS 37008.

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

La organización debe determinar:

a) qué necesita seguimiento y medición;

b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;

c) cuándo se deben llevar a cabo el seguimiento y la medición;

d) cuándo se deben analizar y evaluar los resultados del seguimiento y la medición;

Debe estar disponible la información documentada como evidencia de los resultados.

La organización debe evaluar el desempeño en relación con el antisoborno y la eficacia del sistema de gestión antisoborno.

NOTA Véase el Capítulo A.19 para orientación.

9.2 Auditoría interna

9.2.1 Generalidades

La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión antisoborno:

a) es conforme con:

   1) los requisitos propios de la organización para su sistema de gestión antisoborno;

   2) los requisitos de este documento;

b) se implementa y mantiene eficazmente.

NOTA 1 Se brinda orientación sobre auditoría de sistemas de gestión en la Norma ISO 19011.

NOTA 2 El alcance y la escala de las actividades de auditoría interna de la organización pueden variar dependiendo de una variedad de factores, incluyendo el tamaño de la organización, la estructura, la madurez y ubicaciones.

NOTA 3 Véase el Capítulo A.16 para orientación.

9.2.2 Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Al establecer los programas de auditoría interna, la organización debe considerar la importancia de los procesos involucrados y los resultados de auditorías previas.

La organización debe:

a) definir los objetivos, criterios y el alcance de cada auditoría;

b) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

c) asegurarse de que los resultados de las auditorías se comunican a las gerencias pertinentes, a la función antisoborno, a la alta dirección y cuando sea apropiado, al órgano de gobierno.

Debe estar disponible la información documentada como evidencia de la implementación de los programas de auditoría y de los resultados de las auditorías.

9.2.3 Procedimientos, controles y sistemas de auditoría

Estas auditorías deben ser razonables, proporcionadas, y basadas en el riesgo. Estas auditorías deben consistir en procesos de auditoría interna u otros procedimientos que revisen los procedimientos, controles y sistemas para:

a) soborno o sospecha de soborno;

b) violación de los requisitos de la política antisoborno o del sistema de gestión antisoborno;

c) fracaso de los socios de negocios en cumplir con los requisitos antisoborno aplicables de la organización;

d) debilidades u oportunidades de mejora en el sistema de gestión antisoborno.

9.2.4 Objetividad e imparcialidad

Para asegurar la objetividad e imparcialidad de esos programas de auditoría, la organización debe asegurarse de que estas auditorías se efectúen por una de las siguientes:

a) una función independiente o por personal establecido o designado para este proceso; o

b) la función antisoborno a menos que el alcance de la auditoría incluya una evaluación del propio sistema de gestión antisoborno, o un trabajo similar del que sea responsable la función antisoborno; o

c) una persona apropiada de un departamento o función distintos del que está siendo auditado; o

d) una tercera parte apropiada; o

e) un grupo que comprenda cualquiera de a) a d).

La organización debe asegurarse de que ningún auditor esté realizando la auditoría de su propia área de trabajo.

9.3 Revisión por la dirección

9.3.1 Generalidades

La alta dirección debe revisar el sistema de gestión antisoborno de la organización a intervalos planificados, para asegurarse de su idoneidad, adecuación y eficacia continuas.

El órgano de gobierno debe realizar revisiones de la implementación del sistema de gestión antisoborno por parte de la alta dirección, a intervalos planificados, basándose en la información proporcionada por la alta dirección y la función antisoborno y cualquier otra información que el órgano de gobierno solicite u obtenga.

9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección debe incluir:

a) el estado de las acciones de las revisiones por la dirección previas;

b) los cambios en las cuestiones externas e internas que sean pertinentes para el sistema de gestión antisoborno;

c) los cambios en las necesidades y las expectativas de las partes interesadas que sean pertinentes para el sistema de gestión antisoborno;

d) la información sobre el desempeño del sistema de gestión antisoborno, incluidas las tendencias relativas a:

   1) no conformidades y acciones correctivas;

   2) resultados de seguimiento y medición;

   3) resultados de las auditorías;

   4) informes de sobornos;

   5) investigaciones;

   6) la naturaleza y extensión de los riesgos de soborno a los que se enfrenta la organización;

e) las oportunidades de mejora continua;

f) la eficacia de las medidas adoptadas para abordar los riesgos de soborno;

9.3.3 Resultados de la revisión por la dirección

Los resultados de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión antisoborno.

Debe estar disponible la información documentada para proporcionar evidencia de los resultados de las revisiones por la dirección.

Un resumen de los resultados de la revisión por la dirección se debe informar al órgano de gobierno.

9.4 Revisión por la función antisoborno

La función antisoborno debe evaluar de forma continua si el sistema de gestión antisoborno:

a) es adecuado para gestionar eficazmente los riesgos de soborno a los que se enfrenta la organización;

b) está siendo implementado de manera eficaz.

La función antisoborno debe informar a intervalos planificados y sobre una base *ad hoc*, cuando sea apropiado, al órgano de gobierno y a la alta dirección, o a un comité apropiado del órgano de gobierno o de la alta dirección, sobre la adecuación y la implementación del sistema de gestión antisoborno, incluyendo los resultados de las investigaciones y auditorías.

NOTA 1 La frecuencia de tales informes depende de la estructura y las necesidades de la organización.

NOTA 2 La organización puede usar un socio de negocios para ayudar en la revisión, siempre y cuando las observaciones del socio de negocios se comuniquen adecuadamente a la función antisoborno, a la alta dirección y si es apropiado, al órgano de gobierno.

10 Mejora

10.1 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación, y eficacia del sistema de gestión antisoborno.

NOTA Véase el Capítulo A.20 para orientación.

10.2 No conformidad y acción correctiva

Cuando ocurre una no conformidad, la organización debe:

a) reaccionar ante la no conformidad y, según sea aplicable:

   1) tomar acciones para controlarla y corregirla;

   2) hacer frente a las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:

   1) la revisión de la no conformidad;

   2) la determinación de las causas de la no conformidad;

   3) la determinación de si existen no conformidades similares, o que podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de cualquier acción correctiva tomada;

e) si es necesario, hacer cambios en el sistema de gestión antisoborno.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

Debe estar disponible la información documentada como evidencia de:

— la naturaleza de las no conformidades y cualquier acción tomada posteriormente;

— los resultados de cualquier acción correctiva.

NOTA Véase el Capítulo A.20 para orientación.

Anexo A
(informativo)

Orientación sobre el uso de este documento

A.1 Generalidades

La orientación en este Anexo es solamente ilustrativa. Su finalidad es indicar, en algunas áreas específicas, el tipo de acciones que una organización puede tomar en la implementación de su sistema de gestión antisoborno. Este no pretende ser exhaustivo ni prescriptivo, ni es requerido que una organización implemente las siguientes medidas con el fin de tener un sistema de gestión antisoborno que cumpla con los requisitos de este documento. Los pasos dados por la organización deberían ser razonables y proporcionales teniendo en cuenta la naturaleza y alcance de los riesgos de soborno que enfrenta la organización (véase 4.5, y los factores en 4.1 y 4.2).

Se brinda mayor orientación sobre buenas prácticas en gestión antisoborno en las publicaciones listadas en la Bibliografía.

A.2 Alcance del sistema de gestión antisoborno

A.2.1 Sistema de gestión antisoborno independiente o integrado

La organización puede optar por implementar este sistema de gestión antisoborno como un sistema independiente o como parte integrante de un sistema general de gestión de *compliance* (en cuyo caso, la organización puede consultar para orientación la Norma ISO 37301). La organización también puede optar por implementar este sistema de gestión antisoborno en paralelo a, o como parte de, sus otros sistemas de gestión, como los de gestión de la calidad, gestión ambiental y gestión de la seguridad de la información (en cuyo caso la organización puede referirse a las Normas ISO 9001, ISO 14001, e ISO/IEC 27001), así como ISO 26000 e ISO 31000.

A.2.2 Pagos de facilitación y extorsión

A.2.2.1 Pagos de facilitación es el término que se da a veces a un pago ilegal o no oficial realizado a cambio de servicios que el pagador está legalmente autorizado para recibir sin realizar dicho pago. Normalmente es un pago relativamente menor hecho a un funcionario público o una persona con una función de certificación con el fin de asegurar o agilizar el curso de un trámite o acción necesaria, tales como la emisión de una visa, permiso de trabajo, despacho de aduanas o la instalación de un teléfono. A pesar de que los pagos de facilitación son a menudo considerados como de naturaleza diferente a, por ejemplo, un soborno pagado para obtener negocios, son ilegales en la mayoría de lugares, y son tratados como sobornos a los efectos de este documento y, por lo tanto, debería prohibirse por el sistema de gestión antisoborno de la organización.

A.2.2.2 Un pago de extorsión se presenta cuando el dinero es extraído por la fuerza por parte del personal por amenazas reales o percibidas contra la salud, la seguridad o la libertad y está fuera del alcance de este documento. La seguridad y la libertad de una persona es de suma importancia y muchos sistemas legales no penalizan que alguien que tema razonablemente por su propia salud, seguridad o libertad, o la de otra persona, realice un pago. Por lo tanto, la organización puede tener una política para permitir un pago por parte del personal en circunstancias en las que este tenga miedo al peligro inminente por su propia salud, seguridad o libertad o la de otra persona.

A.2.2.3 La organización debería proporcionar a cualquier miembro del personal al que se le hayan presentado solicitudes o demandas de pago, orientación específica sobre cómo evitarlos y tratar con ellos. Dicha orientación puede incluir, por ejemplo:

a) especificar la acción a adoptar por cualquier miembro del personal que se enfrente con una demanda de pago:

   1) en el caso de un pago de facilitación, pedir una prueba de que el pago es legítimo, y un recibo oficial de pago y, si no hay una prueba satisfactoria disponible, negarse a hacer el pago;

   2) en el caso de un pago de la extorsión, hacer el pago si su salud, seguridad o libertad, o la de otro, se ve amenazada;

b) especificar la acción a adoptar por el personal que haya hecho un pago de facilitación o extorsión:

   1) hacer un registro del evento;

   2) informar del hecho a un gerente apropiado o a la función antisoborno;

c) especificar la acción a adoptar por la organización cuando el personal haya hecho un pago de facilitación o extorsión:

   1) nombrar a un gerente adecuado para investigar el evento (preferentemente la función antisoborno o un gerente que es independiente del personal del departamento o función);

   2) registrar correctamente el pago en cuentas de la organización;

   3) en su caso, o si es requerido por la ley, informar del pago a las autoridades pertinentes.

A.3 Sistema de gestión antisoborno

A.3.1 El soborno suele estar oculto. Puede ser difícil prevenirlo, detectarlo y responder a él. Reconociendo estas dificultades, la intención general de este documento es que el órgano de gobierno y la alta dirección de una organización:

— tengan un compromiso genuino de prevenir, detectar y responder al soborno en relación con el negocio o las actividades de la organización;

— con una intención genuina, implementen medidas en la organización diseñadas para prevenir, detectar y responder al soborno.

A.3.2 Las medidas no pueden ser tan costosas, pesadas y burocráticas que sean inaccesibles o paralicen el negocio, ni pueden ser tan simples e ineficaces que el soborno pueda ocurrir fácilmente. Las medidas necesitan ser apropiadas al riesgo de soborno y deberían tener una probabilidad razonable de tener éxito en su objetivo de prevenir, detectar y responder al soborno.

A.3.3 Si bien los tipos de medidas relacionadas con el antisoborno que necesitan implementarse están razonablemente bien reconocidos por las buenas prácticas internacionales, y algunas de las cuales se reflejan como requisitos en este documento, los detalles de las medidas que deberían implementarse difieren ampliamente según las circunstancias pertinentes. Es imposible prescribir en detalle lo que una organización debería realizar en cualquier circunstancia particular. La calificación de “razonable y proporcionado” se ha introducido en este documento, de modo que cada circunstancia pueda juzgarse por sus propios méritos.

A.3.4 Los siguientes ejemplos brindan cierta orientación sobre cómo puede aplicarse la calificación de “razonable y proporcionado” en relación con diferentes circunstancias.

a) Una organización multinacional muy grande necesita lidiar con múltiples niveles de gestión y miles de personas. Su sistema de gestión antisoborno normalmente necesitará ser mucho más detallado que el de una organización pequeña con solo unas pocas personas.

b) Una organización que desarrolla actividades en un lugar con un riesgo de soborno más alto normalmente necesitará una evaluación del riesgo de soborno y procedimientos de debida diligencia más completos y un nivel más alto de control antisoborno sobre sus transacciones comerciales en ese lugar que una organización que solo desarrolla actividades en un lugar con un riesgo de soborno más bajo, donde el soborno es relativamente poco frecuente.

c) Aunque el riesgo de soborno existe en relación con muchas transacciones o actividades, la evaluación del riesgo de soborno, los procedimientos de debida diligencia y los controles antisoborno implementados por una organización involucrada en una transacción o actividades de gran valor que involucran a una amplia gama de socios de negocios probablemente sean más completos que los implementados por una organización en relación con un negocio que involucra la venta de artículos de poco valor a múltiples clientes o múltiples transacciones más pequeñas con una sola parte.

d) Una organización con una gama muy amplia de socios de negocios puede concluir, como parte de su evaluación del riesgo de soborno, que es poco probable que ciertas categorías de socios de negocios, por ejemplo, los clientes minoristas, representen más que un riesgo bajo de soborno, y tener eso en cuenta en el diseño e implementación de su sistema de gestión antisoborno. Por ejemplo, es poco probable que la debida diligencia sea necesaria, o que sea un control proporcionado y razonable, en relación con los clientes minoristas que compran artículos tales como bienes de consumo de la organización.

A.3.5 Aunque el riesgo de soborno existe en relación con muchas transacciones, una organización debería implementar un nivel más integral de control antisoborno sobre una transacción de alto riesgo de soborno que sobre una transacción de bajo riesgo de soborno. En este contexto, es importante entender que identificar y aceptar un bajo riesgo de soborno no significa que la organización acepte el hecho de que ocurra un soborno, es decir, el riesgo de que ocurra un soborno (si puede ocurrir un soborno) no es lo mismo que la ocurrencia de un soborno (el hecho del soborno en sí). Una organización puede tener una “tolerancia cero” para la ocurrencia de un soborno mientras siga realizando negocios en situaciones en las que puede haber un bajo riesgo de soborno, o más que un riesgo bajo de soborno (siempre que se apliquen medidas de mitigación adecuadas). A continuación se proporciona más orientación sobre controles específicos.

A.4 Evaluación del riesgo de soborno

A.4.1 La intención de la evaluación del riesgo de soborno requerida en el apartado 4.5 es permitir que la organización forme una base sólida para su sistema de gestión antisoborno. Esta evaluación identifica los riesgos de soborno en los que se centrará el sistema de gestión, es decir, los riesgos de soborno que la organización considera prioritarios para la mitigación del riesgo de soborno, la implementación de controles y la asignación de personal, recursos y actividades de cumplimiento antisoborno. La forma en que la organización lleva a cabo la evaluación del riesgo de soborno, la metodología que emplea, cómo se ponderan y priorizan los riesgos de soborno y el nivel de riesgo de soborno que se acepta (es decir, "apetito de riesgo") o se tolera, son todos a discreción de la organización. En particular, es la organización la que establece sus criterios para evaluar el riesgo de soborno (por ejemplo, si un riesgo es "bajo", "medio" o "alto"); sin embargo, al hacerlo, la organización debería tener en cuenta su política y sus objetivos antisoborno.

A.4.2 El siguiente es un ejemplo de cómo una organización puede optar por llevar a cabo esta evaluación:

a) Seleccionar criterios de evaluación del riesgo de soborno. Por ejemplo, la organización puede seleccionar criterios de tres niveles (por ejemplo, “bajo”, “medio”, “alto”), criterios más detallados de cinco o siete niveles, o un enfoque más detallado. Los criterios a menudo tendrán en cuenta varios factores, incluida la naturaleza del riesgo de soborno, la probabilidad de que ocurra el soborno y la magnitud de las consecuencias en caso de que ocurra.

b) Evaluar los riesgos de soborno que representan el tamaño y la estructura de la organización. Una organización pequeña con sede en una ubicación con controles de gestión centralizados en manos de unas pocas personas puede controlar su riesgo de soborno más fácilmente que una organización muy grande con una estructura descentralizada que opera en muchas ubicaciones.

c) Examinar las ubicaciones y los sectores en los que la organización opera o prevé operar, y evaluar el nivel de riesgo de soborno que pueden representar estas ubicaciones y sectores. Se puede utilizar un índice de soborno adecuado para ayudar en esta evaluación. Las ubicaciones o sectores con un mayor riesgo de soborno pueden ser considerados por la organización como de riesgo "medio" o "alto", por ejemplo, lo que puede dar lugar a que la organización imponga un mayor nivel de controles aplicables a las actividades de la organización en esas ubicaciones o sectores.

d) Examinar la naturaleza, escala y complejidad de los tipos de actividades y operaciones de la organización:

   1) Por ejemplo, puede ser más fácil controlar el riesgo de soborno cuando una organización lleva a cabo una pequeña operación de fabricación en un lugar que cuando participa en numerosos proyectos de construcción de gran envergadura en varios lugares.

   2) Algunas actividades pueden conllevar riesgos específicos de soborno, por ejemplo, los acuerdos de compensación por los cuales el gobierno que compra productos o servicios exige al proveedor que reinvierta una parte del valor del contrato en el país comprador. La organización debería tomar las medidas adecuadas para evitar que los acuerdos de compensación constituyan soborno.

e) Examinar los tipos de socios de negocios existentes y potenciales de la organización por categoría y evaluar el riesgo de soborno que en principio representan. Por ejemplo:

   1) La organización puede tener un gran número de clientes que compran productos de muy bajo valor de la organización y que en la práctica representan un riesgo mínimo de soborno para la organización. En este caso, la organización puede considerar que estos clientes presentan un riesgo bajo de soborno y puede determinar que no será necesario aplicar controles específicos contra el soborno a estos clientes. Otra posibilidad es que la organización trate con clientes que compran productos de gran valor y que pueden representar un riesgo de soborno significativo (por ejemplo, el riesgo de exigir sobornos a la organización a cambio de pagos o aprobaciones). Estos tipos de clientes pueden considerarse de riesgo de soborno "medio" o "alto" y pueden requerir un nivel más alto de controles antisoborno por parte de la organización.

   2) Las distintas categorías de proveedores pueden representar distintos niveles de riesgo de soborno. Por ejemplo, los proveedores con un alcance de trabajo muy amplio, o que pueden estar en contacto con los clientes de la organización, consumidores o funcionarios públicos relevantes, pueden representar un riesgo de soborno "medio" o "alto". Algunas categorías de proveedores pueden ser un riesgo "bajo", por ejemplo, los proveedores con sede en lugares de bajo riesgo de soborno que no tienen interacción con funcionarios públicos pertinentes para la transacción o con los clientes de la organización. Algunas categorías de proveedores pueden representar un riesgo de soborno "muy bajo", por ejemplo, los proveedores de pequeñas cantidades de artículos de bajo valor, servicios de compra en línea de viajes aéreos u hoteles. La organización puede concluir que no es necesario implementar controles antisoborno específicos en relación con estos proveedores de riesgo de soborno bajo o muy bajo.

   3) Los agentes o intermediarios que interactúan con los clientes de la organización o funcionarios públicos en nombre de la organización probablemente representen un riesgo de soborno "medio" o "alto", en particular si se les paga en base a una comisión o a un honorario por éxito.

f) Examinar la naturaleza y frecuencia de las interacciones con funcionarios públicos nacionales o extranjeros que puedan representar un riesgo de soborno, por ejemplo, las interacciones con funcionarios públicos responsables de emitir permisos y aprobaciones pueden representar un riesgo de soborno.

g) Examinar las obligaciones y deberes legales, reglamentarios, contractuales y profesionales aplicables, por ejemplo, la prohibición o limitación de las invitaciones a funcionarios públicos o del uso de agentes.

h) Considerar hasta qué punto la organización puede influir o controlar los riesgos evaluados.

A.4.3 Los factores de riesgo de soborno anteriores están interrelacionados. Por ejemplo, los proveedores de la misma categoría pueden representar un riesgo de soborno diferente según el lugar en el que operen.

A.4.4 Una vez evaluados los riesgos de soborno pertinentes, la organización puede determinar el tipo y nivel de controles antisoborno que se aplican a cada categoría de riesgo y puede evaluar si los controles existentes son adecuados. En caso contrario, los controles se pueden mejorar de forma adecuada. Por ejemplo, es probable que se implemente un nivel más alto de control con respecto a lugares con mayor riesgo de soborno y categorías de socios de negocios con mayor riesgo de soborno. La organización puede determinar que es aceptable tener un nivel bajo de control sobre actividades o socios de negocios con bajo riesgo de soborno. Algunos de los requisitos de este documento excluyen expresamente la necesidad de aplicar esos requisitos a actividades o socios de negocios con bajo riesgo de soborno (aunque la organización puede optar por aplicarlos si lo desea).

A.4.5 La organización puede cambiar la naturaleza de la transacción, proyecto, actividad o relación de modo que la naturaleza y el alcance del riesgo de soborno se reduzcan a un nivel que pueda gestionarse adecuadamente mediante controles antisoborno existentes, mejorados o adicionales.

A.4.6 Este ejercicio de evaluación del riesgo de soborno no pretende ser un ejercicio extenso o excesivamente complejo, y los resultados de la evaluación no necesariamente resultarán correctos (por ejemplo, una transacción evaluada como de bajo riesgo de soborno puede resultar haber involucrado soborno). En la medida de lo razonablemente posible, los resultados de la evaluación del riesgo de soborno deberían reflejar los riesgos de soborno reales a los que se enfrenta la organización. El ejercicio debería diseñarse como una herramienta para ayudar a la organización a evaluar y priorizar su riesgo de soborno, y debería revisar a intervalos planificados y modificarse en función de los cambios en la organización o las circunstancias (por ejemplo, nuevos mercados o productos, requisitos legales, experiencias adquiridas).

NOTA Se proporciona orientación adicional en las Normas ISO 31000 e ISO 31022.

A.5 Roles y responsabilidades del órgano de gobierno y de la alta dirección

A.5.1 Generalidades

A.5.1.1 Muchas organizaciones cuentan con algún tipo de órgano de gobierno (por ejemplo, un consejo de administración o un consejo de supervisión) que tiene responsabilidades generales de supervisión con respecto a la organización. Estas responsabilidades incluyen la supervisión del sistema de gestión antisoborno de la organización. Sin embargo, el órgano de gobierno generalmente no ejerce una dirección diaria sobre las actividades de la organización. Ése es el rol de la dirección ejecutiva (por ejemplo, el director ejecutivo, el director de operaciones), a la que se hace referencia en este documento como “alta dirección”. Con respecto al sistema de gestión antisoborno, el órgano de gobierno debería conocer el contenido y el funcionamiento del sistema de gestión, y debería ejercer una supervisión razonable con respecto a la adecuación, la eficacia y la implementación del sistema de gestión. Debería recibir información a intervalos planificados sobre el desempeño del sistema de gestión a través del proceso de revisión de la dirección (puede ser para todo el órgano de gobierno o para un comité del órgano, como el comité de auditoría). En este sentido, la función antisoborno debería poder informar sobre el sistema de gestión directamente al órgano de gobierno (o al comité correspondiente del mismo).

A.5.1.2 Es posible que algunas organizaciones, en particular las más pequeñas, no tengan un órgano de gobierno separado, o que los roles del órgano de gobierno y la dirección ejecutiva se combinen en un grupo o incluso en una sola persona. En tales casos, el grupo o la persona tendrán las responsabilidades asignadas en este documento a la alta dirección y al órgano de gobierno.

NOTA El compromiso del liderazgo a veces se denomina «tono en la cúspide» (*tone of the top*) o «tono desde la cúspide» (*tone from the top*).

A.5.2 Cultura antisoborno

A.5.2.1 Los factores que apoyan el desarrollo de una cultura antisoborno incluyen:

— una dirección que implementa, promueve y respeta activa y visiblemente la cultura antisoborno de la organización;

— la tutoría y el liderazgo con el ejemplo sobre la importancia de la cultura antisoborno de la organización;

— un énfasis en la cultura antisoborno de la organización en el programa de inducción para el personal;

— la comunicación continua con el personal sobre la cultura antisoborno de la organización;

— el reconocimiento visible de los logros del personal en la promoción de la cultura antisoborno de la organización;

— la consistencia en el tratamiento de las conductas del personal que comprometan la cultura antisoborno de la organización, independientemente del puesto que ocupe.

A.5.2.2 La evidencia de una cultura antisoborno se demuestra por el grado en que:

— los elementos anteriores están documentados, implementados y practicados;

— el personal cree que los elementos anteriores se han implementado;

— el personal entiende la relevancia de la cultura antisoborno de la organización para su puesto, sus propias actividades y las de su unidad de negocios;

— el personal valora el rol y los objetivos del sistema de gestión antisoborno, en particular de la política antisoborno, de los procedimientos relacionados y de la función antisoborno;

— las acciones correctivas para abordar el comportamiento del personal que compromete el sistema de gestión antisoborno de la organización son “asumidas” y ejecutadas, según sea necesario, en todos los niveles adecuados de la organización.

A.6 Función antisoborno

A.6.1 La cantidad de personas que trabajan en la función antisoborno depende de factores como el tamaño de la organización, el grado de riesgo de soborno que enfrenta la organización y la carga de trabajo resultante de la función. En una organización pequeña, es probable que la función antisoborno esté a cargo de una persona a la que se le asigne la responsabilidad a tiempo parcial y que combine esta responsabilidad con otras responsabilidades. Cuando el grado de riesgo de soborno y la carga de trabajo resultante lo justifiquen, la función antisoborno puede estar a cargo de una persona a la que se le asigne la responsabilidad a tiempo completo. En organizaciones grandes, es probable que la función esté compuesta por varias personas. Algunas organizaciones pueden asignar la responsabilidad a un comité que incorpore una gama de conocimientos especializados pertinentes. Algunas organizaciones pueden optar por utilizar a un tercero para que se encargue de parte o de la totalidad de la función antisoborno, y esto es aceptable siempre que un gerente apropiado dentro de la organización conserve la responsabilidad general y la autoridad sobre la función antisoborno y supervise los servicios prestados por el tercero.

A.6.2 Este documento requiere que la función antisoborno esté compuesta por personas que tengan la competencia, el estatus, la autoridad y la independencia adecuados. En este sentido:

a) “competencia” significa que las personas pertinentes tienen la educación, la formación o la experiencia adecuadas, la capacidad personal para hacer frente a los requisitos del rol y la capacidad de aprender sobre el rol y desempeñarlo adecuadamente;

b) “estatus” significa que es probable que el resto del personal escuche y respete las opiniones de la persona a la que se le ha asignado la responsabilidad de *compliance*;

c) "autoridad" significa que las personas pertinentes a la que se ha asignado la responsabilidad de *compliance* tienen poderes suficientes otorgados por el órgano de gobierno y la alta dirección para poder llevar a cabo las responsabilidades de *compliance* de manera eficaz;

d) "independencia" significa que las personas pertinentes a la que se ha asignado la responsabilidad de *compliance* no están involucradas personalmente, en la medida de lo posible, en las actividades de la organización que están expuestas al riesgo de soborno. Esto se puede lograr más fácilmente cuando la organización ha designado a una persona para que se ocupe del rol a tiempo completo, pero es más difícil para una organización más pequeña que ha designado a una persona para que combine el rol de *compliance* con otras funciones. Cuando la función antisoborno se realiza a tiempo parcial, el rol no debería ser desempeñado por una persona que pueda estar expuesta a sobornos mientras realiza su función principal. En el caso de una organización muy pequeña en la que puede resultar más difícil lograr la independencia, la persona adecuada debería, en la medida de sus posibilidades, separar sus otras responsabilidades de sus responsabilidades de *compliance* para ser imparcial.

A.6.3 Es importante que la función antisoborno tenga acceso directo a la alta dirección y al órgano de gobierno, a fin de comunicar información pertinente. La función no debería tener que reportar únicamente a otro gerente en la cadena que a su vez reporte a la alta dirección, ya que esto aumenta el riesgo de que el mensaje dado por la función antisoborno no sea recibido completa o claramente por la alta dirección. La función antisoborno también debería tener una relación de comunicación directa con el órgano de gobierno, sin tener que pasar por la alta dirección. Esto puede ser con el órgano de gobierno plenamente constituido (por ejemplo, una junta directiva o un consejo de supervisión) o puede ser con un comité especialmente delegado del órgano de gobierno o la alta dirección (por ejemplo, un comité de auditoría o de ética).

A.6.4 La responsabilidad principal de la función antisoborno es supervisar el diseño y la implementación del sistema de gestión antisoborno. Esto no debería confundirse con la responsabilidad directa por el desempeño en relación con el antisoborno de la organización y el cumplimiento de las leyes antisoborno aplicables. Todos son responsables de comportarse de manera ética y conforme a las normas, lo que incluye cumplir con los requisitos del sistema de gestión antisoborno de la organización y las leyes antisoborno. Es especialmente importante que la dirección asuma el rol de liderazgo en el logro del *compliance* en las partes de la organización de las que es responsable.

NOTA Se proporciona más orientación en la Norma ISO 37301.

A.7 Recursos

Los recursos necesarios dependen de factores como el tamaño de la organización, la naturaleza de sus operaciones y los riesgos de soborno a los que se enfrenta. Algunos ejemplos de recursos son los siguientes:

a) Recursos humanos: debería haber suficiente personal que pueda dedicar el tiempo suficiente a sus responsabilidades pertinentes relacionadas con el antisoborno para que el sistema de gestión antisoborno pueda funcionar de manera eficaz. Esto incluye la asignación de una o más personas (internas o externas) suficientes a la función antisoborno.

b) Recursos físicos: debería contar con los recursos físicos necesarios en la organización, incluida la función antisoborno, para que el sistema de gestión antisoborno funcione de manera eficaz, por ejemplo, espacio de oficina, mobiliario, hardware y software informático, materiales de formación, teléfonos, material de oficina.

c) Recursos financieros: debería tener un presupuesto suficiente, incluida la función antisoborno, para que el sistema de gestión antisoborno funcione de manera eficaz.

A.8 Procedimientos de contratación

A.8.1 Debida diligencia con el personal

Al llevar a cabo la debida diligencia con las personas antes de nombrarlas como personal, la organización, dependiendo de las funciones propuestas de las personas y el riesgo de soborno correspondiente, puede tomar medidas como:

a) discutir la política antisoborno de la organización con el personal potencial en la entrevista y formarse una opinión sobre si parecen entender y aceptar la importancia del *compliance*;

b) tomar medidas razonables para verificar que las calificaciones del personal potencial sean precisas;

c) tomar medidas razonables para obtener referencias satisfactorias de los empleadores anteriores del personal potencial;

d) tomar medidas razonables para determinar si el personal potencial ha estado involucrado en sobornos;

e) tomar medidas razonables para verificar que la organización no esté ofreciendo empleo al personal potencial a cambio de que, en empleos anteriores, haya favorecido indebidamente a la organización;

f) verificar que el propósito de ofrecer empleo al personal potencial no sea asegurar un trato favorable indebido para la organización;

g) tomar medidas razonables para identificar la relación del personal potencial con funcionarios públicos.

A.8.2 Bonificaciones por desempeño

A.8.2.1 Los acuerdos de remuneración, incluidas las bonificaciones e incentivos, pueden alentar, incluso de manera involuntaria, al personal a participar en sobornos. Por ejemplo, si un gerente recibe una bonificación en función de la adjudicación de un contrato a la organización, el gerente puede verse tentado a pagar un soborno o a hacer la vista gorda ante un agente o socio de una alianza empresarial que pague un soborno, a fin de asegurar la adjudicación del contrato. El mismo resultado puede ocurrir si se ejerce demasiada presión sobre un gerente para que cumpla con sus funciones (por ejemplo, si el gerente puede ser despedido por no lograr objetivos de ventas demasiado ambiciosos). La organización necesita prestar mucha atención a estos aspectos de la compensación para asegurar, en la medida de lo razonable, que no actúen como incentivos para el soborno.

A.8.2.2 Las evaluaciones del personal, las promociones, las bonificaciones y otras recompensas pueden utilizarse como incentivos para que el personal cumpla con las políticas y el sistema de gestión antisoborno de la organización. Sin embargo, la organización debería ser cautelosa en este caso, ya que la amenaza de pérdida de bonificaciones, etc. puede hacer que el personal oculte fallas en el sistema de gestión antisoborno.

A.8.2.3 Se debería concientizar al personal de que violar el sistema de gestión antisoborno para mejorar su calificación de desempeño en otras áreas (por ejemplo, lograr un objetivo de ventas) no es aceptable y debería dar lugar a medidas correctivas y/o disciplinarias.

A.8.3 Conflictos de interés

A.8.3.1 La organización debería identificar, analizar y evaluar los riesgos de conflictos de interés internos y externos. La organización debería informar claramente a todo el personal de su deber de informar sobre cualquier conflicto de interés potencial o real, como por ejemplo, familiares, financieros u otros vínculos relacionados directa o indirectamente con su línea de trabajo. Esto ayuda a la organización a identificar situaciones en las que el personal puede facilitar o no prevenir o informar sobre el soborno, por ejemplo,

a) cuando el gerente de ventas de la organización está relacionado con el gerente de compras de un cliente,

b) cuando un gerente en una función de compras tiene un interés financiero en un proveedor,

c) cuando el gerente de línea de una organización tiene un interés financiero personal en el negocio de un competidor,

d) cuando un director de una organización (que puede tener un rol no ejecutivo) o un miembro de la alta dirección tiene intereses personales legítimos u ocultos o un puesto en una organización competidora o potencialmente adquirente.

A.8.3.2 La organización debería mantener un registro de todas las declaraciones de conflicto de interés y de cualquier circunstancia de conflicto de interés real o potencial, y de si se tomaron medidas para mitigar el conflicto y cuáles fueron.

A.8.3.3 Estas medidas deberían revisarse al menos una vez al año para asegurar que sigan siendo pertinentes y estén actualizadas.

A.8.4 Soborno del personal de la organización

A.8.4.1 Las medidas necesarias para prevenir, detectar y abordar el riesgo de que el personal de la organización soborne a otros en nombre de la organización ("soborno saliente") pueden ser diferentes de las medidas utilizadas para prevenir, detectar y abordar el riesgo de soborno del personal de la organización ("soborno entrante"). Por ejemplo, la capacidad para identificar y mitigar el riesgo de soborno entrante puede verse significativamente restringida por la disponibilidad de información que no está bajo el control de la organización (por ejemplo, datos de transacciones con tarjetas de crédito y cuentas bancarias personales de empleados), la legislación aplicable (por ejemplo, la ley de privacidad) u otros factores. Como resultado, la cantidad y los tipos de controles disponibles para la organización para mitigar el riesgo de soborno saliente pueden superar la cantidad de controles que puede implementar para mitigar el riesgo de soborno entrante.

A.8.4.2 Es más probable que el soborno del personal de la organización ocurra en relación con el personal que puede tomar decisiones o influir en ellas en nombre de la organización (por ejemplo, un gerente de compras que puede adjudicar contratos; un supervisor que puede aprobar el trabajo realizado; un gerente que puede designar personal o aprobar salarios o bonificaciones; un empleado que prepara documentos para otorgar licencias y permisos). Como es probable que el soborno sea aceptado por personal fuera del alcance de los sistemas o controles de la organización, la capacidad de la organización para prevenir o detectar estos sobornos puede ser limitada.

A.8.4.3 Además de los pasos mencionados en los párrafos sobre debida diligencia y conflicto de interés anteriores, el riesgo de soborno entrante puede mitigarse mediante los siguientes requisitos de este documento que abordan este riesgo:

a) la política antisoborno de la organización (véase 5.2) debería prohibir claramente la solicitud y aceptación de sobornos por parte del personal de la organización y de cualquier persona que trabaje en nombre de la organización;

b) los materiales de orientación y formación (véase 7.3) debería reforzar la prohibición de solicitar y aceptar sobornos e incluir:

   1) orientación para informar sobre inquietudes relacionadas con sobornos (véase 8.9);

   2) énfasis en la política de no represalias de la organización (véase 8.9);

c) la política de obsequios y hospitalidad de la organización (véase 8.7) debería limitar la aceptación de obsequios y hospitalidad por parte del personal;

d) la publicación en el sitio web de la organización de la política antisoborno de la organización y de los detalles sobre cómo informar el soborno ayuda a establecer expectativas con los socios de negocios, como forma de disminuir la probabilidad de que los socios de negocios ofrezcan, o el personal de la organización solicite o acepte, un soborno;

e) los controles (véase 8.3 y 8.4) que requieren, por ejemplo, el uso de proveedores aprobados, licitación competitiva, al menos dos firmas en las adjudicaciones de contratos, aprobaciones de trabajo, etc. reducen el riesgo de adjudicaciones, aprobaciones, pagos o beneficios corruptos.

A.8.4.4 La organización también puede implementar procedimientos de auditoría para identificar formas en las que el personal puede explotar las debilidades de control existentes para obtener ganancias personales. Algunos procedimientos de ejemplo incluyen:

a) revisar los archivos de nómina para detectar registros de personal fantasmas y duplicados;

b) revisar los registros de gastos comerciales del personal para identificar gastos inusuales;

c) comparar la información del archivo de nómina del personal (por ejemplo, números de cuenta bancaria y direcciones personales) con la información de la cuenta bancaria y la dirección en el archivo maestro de proveedores de la organización para identificar posibles escenarios de conflicto de interés.

A.8.5 Personal o trabajadores temporales

En algunos casos, el personal o los trabajadores temporales son proporcionados a la organización por un proveedor de mano de obra u otro socio de negocios. En este caso, la organización debería determinar si el riesgo de soborno que representan dichos trabajadores o empleados temporales (si lo hubiera) se aborda adecuadamente tratando al personal o los trabajadores temporales como su propio personal a efectos de formación y control, o si se imponen controles apropiados a través del socio de negocios que proporciona el personal o los trabajadores temporales.

A.9 Toma de conciencia y formación

A.9.1 La intención de la formación es ayudar a asegurar que el personal pertinente comprenda, según corresponda a su rol en la organización o con ella, lo siguiente:

a) los riesgos de soborno a los que ellos y su organización se enfrentan;

b) la política antisoborno;

c) los aspectos del sistema de gestión antisoborno pertinentes a su rol;

d) cualquier acción preventiva y de reporte necesaria que precisen tomar en relación con cualquier riesgo de soborno o sospecha de soborno.

A.9.2 La formalidad y el alcance de la formación dependen del tamaño de la organización y de los riesgos de soborno a los que se enfrenta. Puede realizarse como un módulo en línea o mediante métodos presenciales (por ejemplo, sesiones en el aula, talleres, mesas redondas entre el personal pertinente o sesiones individuales). El método de la formación es menos importante que el resultado, que es que todo el personal pertinente comprenda los asuntos a los que se hace referencia en el apartado A.9.1.

A.9.3 Se recomienda la formación presencial para el órgano de gobierno y para todo el personal (independientemente de sus puestos o jerarquía dentro de la organización) y los socios de negocios que estén involucrados en operaciones y procesos con más que un riesgo bajo de soborno.

A.9.4 Si las personas pertinentes asignadas a la función antisoborno no tienen suficiente experiencia relacionada, la organización debería proporcionarle la formación necesaria para que desempeñe la función antisoborno de manera adecuada.

A.9.5 La formación puede realizarse como formación antisoborno independiente o puede ser parte del programa general de formación o inducción en *compliance* y ética de la organización.

A.9.6 El contenido de la formación puede adaptarse al rol del personal. El personal que no enfrenta ningún riesgo significativo de soborno en su rol puede recibir una formación muy simple sobre la política de la organización, de modo que comprenda la política y sepa qué hacer si ve una posible violación. El personal cuyo rol implica un alto riesgo de soborno debería recibir una formación más detallada.

A.9.7 La formación debería repetirse con la frecuencia necesaria para que el personal esté al día con las políticas y procedimientos de la organización, cualquier desarrollo en relación con su rol y cualquier cambio regulatorio.

A.9.8 La aplicación de los requisitos de formación a los socios de negocios identificados bajo los requisitos del apartado 7.3.4 representa desafíos particulares porque los empleados de dichos socios de negocios generalmente no trabajan directamente para la organización, y la organización normalmente no tendrá acceso directo a dichos empleados para fines de formación. La formación real de los empleados que trabajan para socios de negocios normalmente debería ser realizada por los socios de negocios o por otras partes contratadas para ese propósito. Es importante que los empleados que trabajan para socios de negocios que pueden representar más que un riesgo bajo de soborno para la organización tomen conciencia del asunto y reciban formación razonablemente destinada a reducir este riesgo. El contenido del apartado 7.3.4 requiere que la organización, como mínimo, identifique a los socios de negocios cuyos empleados deberían recibir formación antisoborno, debería ser el contenido mínimo de dicha formación y que dicha formación debería realizarse. La formación en sí puede ser proporcionada por el socio de negocios, por otras partes designadas o, si la organización así lo elige, por la organización. La organización puede comunicar estas obligaciones a sus socios de negocios de diversas maneras, incluso como parte de acuerdos contractuales.

A.10 Debida diligencia

A.10.1 El propósito de realizar la debida diligencia sobre ciertas transacciones, proyectos, actividades, socios de negocios o el personal de una organización es evaluar más a fondo el alcance, la escala y la naturaleza de los riesgos de soborno más que bajos identificados como parte de la evaluación de riesgos de la organización (véase 4.5). También sirve para el propósito de actuar como un control adicional y específico en la prevención y detección del riesgo de soborno, e informa la decisión de la organización sobre si posponer, interrumpir o revisar esas transacciones, proyectos o relaciones con socios de negocios o personal.

A.10.2 En relación con los proyectos, transacciones y actividades, los factores que la organización puede considerar útil evaluar incluyen:

a) estructura, naturaleza y complejidad (por ejemplo, venta directa o indirecta, nivel de descuento, adjudicación de contratos y procedimientos de licitación);

b) los mecanismos de financiación y pago;

c) el alcance del compromiso de la organización y los recursos disponibles;

d) nivel de control y visibilidad;

e) socios de negocios y otras terceras partes involucradas (incluidos funcionarios públicos);

f) vínculos entre cualquiera de las partes mencionadas en el punto e) anterior y funcionarios públicos;

g) competencia y calificaciones de las partes involucradas;

h) reputación del cliente;

i) ubicación;

j) informes en el mercado o en la prensa.

A.10.3 En relación con la posible debida diligencia sobre socios de negocios:

a) los factores que la organización puede considerar útil evaluar en relación con un socio de negocios incluyen:

   1) si el socio de negocios es una entidad comercial legítima, como lo demuestran indicadores como documentos de registro corporativo, cuentas anuales presentadas, número de identificación fiscal, cotización en una bolsa de valores;

   2) si el socio de negocios tiene las calificaciones, la experiencia y los recursos necesarios para llevar a cabo el negocio para el que se lo contrata;

   3) si el socio de negocios tiene un sistema de gestión antisoborno y en qué medida lo tiene;

   4) si el socio de negocios tiene reputación de soborno, fraude, deshonestidad o mala conducta similar, o ha sido investigado, condenado, sancionado o inhabilitado por soborno o conducta delictiva similar;

   5) la identidad de los accionistas (incluido el o los propietarios beneficiarios finales) y la alta gerencia del socio de negocios, y si:

      i) tienen reputación de soborno, fraude, deshonestidad o mala conducta similar;

      ii) han sido investigados, condenados, sancionados o inhabilitados por soborno o conducta delictiva similar;

      iii) tienen vínculos directos o indirectos con el cliente o cliente de la organización o con un funcionario público relevante que puedan dar lugar al soborno (esto incluye a personas que no son funcionarios públicos, pero que pueden estar relacionadas directa o indirectamente con funcionarios públicos, candidatos a cargos públicos, etc.);

   6) la estructura de la transacción y los acuerdos de pago;

b) la naturaleza, el tipo y el alcance de la debida diligencia realizada dependerán de factores como la capacidad de la organización para obtener información suficiente, el costo de obtener información y el alcance del posible riesgo de soborno que representa la relación;

c) los procedimientos de debida diligencia implementados por la organización con sus socios de negocios deberían ser consistentes en niveles similares de riesgo de soborno (es probable que los socios de negocios con alto riesgo de soborno en lugares o mercados donde existe un alto riesgo de soborno requieran un nivel significativamente más alto de debida diligencia que los socios de negocios con menor riesgo de soborno en lugares o mercados con bajo riesgo de soborno);

d) es probable que diferentes tipos de socios de negocios requieran diferentes niveles de debida diligencia, por ejemplo:

   1) desde la perspectiva de una potencial responsabilidad legal y financiera de la organización, los socios de negocios representan un mayor riesgo de soborno para la organización cuando actúan en nombre de la organización o para su beneficio que cuando proporcionan productos o servicios a la organización. Por ejemplo, un agente que ayuda a una organización a obtener la adjudicación de un contrato puede pagar un soborno a un gerente del cliente de la organización para ayudar a la organización a ganar el contrato, y por lo tanto puede resultar en que la organización sea responsable de la conducta corrupta del agente. Como resultado, es probable que la debida diligencia de la organización sobre el agente sea lo más exhaustiva posible. Por otro lado, un proveedor que vende equipo o material a la organización, y que no tiene relación con los clientes de la organización o funcionarios públicos que son pertinentes para las actividades de la organización, tiene menos probabilidades de poder pagar un soborno en nombre de la organización o para su beneficio, y por lo tanto el nivel de debida diligencia sobre el proveedor puede ser menor;

   2) el nivel de influencia que la organización tiene sobre sus socios de negocios también afecta la capacidad de la organización para obtener información directamente de esos socios de negocios como parte de su debida diligencia. Puede ser relativamente fácil para una organización exigir a

sus agentes y alianzas empresariales conjuntas que proporcionen información extensa sobre sí mismos como parte de un ejercicio de debida diligencia antes de que la organización se comprometa a trabajar con ellos, ya que la organización tiene un grado de elección sobre con quién contrata en esta situación. Sin embargo, puede ser más difícil para una organización exigir a un cliente o comprador que proporcione información sobre sí mismo o que complete cuestionarios de debida diligencia. Esto puede ser porque la organización no tendría suficiente influencia sobre el cliente o comprador para poder hacerlo (por ejemplo, cuando la organización participa en una licitación competitiva para proporcionar servicios al cliente);

e) la debida diligencia realizada por la organización sobre sus socios de negocios puede incluir, por ejemplo:

   1) un cuestionario enviado al socio de negocios en el que se le pide que responda las preguntas a las que se hace referencia en el apartado A.10.3 a).

   2) una búsqueda en la web sobre el socio de negocios y sus accionistas y la alta gerencia para identificar cualquier información relacionada con el soborno;

   3) buscar información pertinente en los recursos gubernamentales, judiciales e internacionales apropiados;

   4) verificar las listas de inhabilitación disponibles públicamente de organizaciones que tienen prohibido o restringido contratar con entidades públicas o gubernamentales, mantenidas por gobiernos nacionales o locales o instituciones multilaterales, como el Banco Mundial;

   5) hacer averiguaciones a otras partes apropiadas sobre la reputación ética del socio de negocios;

   6) designar a otras personas u organizaciones con experiencia pertinente para ayudar en el proceso de debida diligencia;

f) se pueden hacer más preguntas al socio de negocios en función de los resultados de la debida diligencia inicial (por ejemplo, para explicar cualquier información adversa).

A.10.4 La debida diligencia no es una herramienta perfecta. La ausencia de información negativa no significa necesariamente que el socio de negocios no represente un riesgo de soborno. La información negativa no significa necesariamente que el socio de negocios represente un riesgo de soborno. Sin embargo, los resultados deberían evaluarse cuidadosamente y la organización debería emitir un juicio racional basado en los hechos disponibles. La intención general es que la organización haga averiguaciones razonables y proporcionadas sobre el socio de negocios, teniendo en cuenta las actividades que el socio de negocios llevaría a cabo y el riesgo de soborno inherente a estas actividades, a fin de formar un juicio razonable sobre el nivel de riesgo de soborno al que está expuesta la organización si trabaja con el socio de negocios.

A.10.5 La debida diligencia sobre el personal se trata en el Capítulo A.8.

A.11 Controles financieros

Los controles financieros son los sistemas y procesos de gestión implementados por la organización para gestionar sus transacciones financieras de forma adecuada y registrar estas transacciones de forma precisa, completa y oportuna. Los controles financieros antisoborno bien diseñados actúan como controles y contrapesos para disuadir el comportamiento indebido al aumentar el riesgo de detección y capturar información para permitir la investigación. Dependiendo del tamaño de la organización y de la transacción, los controles financieros implementados por una organización que pueden reducir el riesgo de soborno pueden incluir, por ejemplo:

a) implementar una separación de funciones, de modo que la misma persona no pueda iniciar y aprobar un pago;

b) implementar niveles de autoridad apropiados para la aprobación de pagos (de modo que las transacciones más grandes requieran la aprobación de un nivel superior de la gerencia);

c) verificar que el nombramiento del beneficiario y el trabajo o los servicios realizados hayan sido aprobados por los mecanismos de aprobación pertinentes de la organización;

d) exigir al menos dos firmas en las aprobaciones de pagos;

e) exigir que se adjunte la documentación de respaldo adecuada a las aprobaciones de pagos;

f) restringir el uso de efectivo e implementar métodos eficaces de control de efectivo;

g) exigir que las categorizaciones y descripciones de los pagos en las cuentas sean precisas y claras;

h) implementar una revisión por parte de la gerencia a intervalos planificados de las transacciones financieras significativas;

i) implementar auditorías financieras independientes a intervalos planificados y cambiar, también a intervalos planificados, la persona o la organización que realiza la auditoría.

A.12 Controles no financieros

Los controles no financieros son los sistemas y procesos de gestión implementados por la organización para ayudarla a asegurar que los aspectos de compras, operacionales, comerciales y otros aspectos no financieros de sus actividades se están gestionando adecuadamente. Dependiendo del tamaño de la organización y de la transacción, los controles de compras, operacionales, comerciales y otros controles no financieros implementados por una organización que pueden reducir el riesgo de soborno pueden incluir, por ejemplo, los siguientes controles:

a) utilizar contratistas, subcontratistas, proveedores y consultores aprobados que hayan pasado por un proceso de precalificación en virtud del cual se evalúa la probabilidad de que participen en un soborno; este proceso probablemente incluya la debida diligencia del tipo especificado en el Capítulo A.10;

b) evaluar:

   1) la necesidad y legitimidad de los servicios que un socio de negocios (excluidos los clientes) prestará a la organización,

   2) si los servicios se llevaron a cabo correctamente;

   3) si los pagos que se realizarán al socio de negocios son razonables y proporcionados con respecto a esos servicios. Esto es particularmente importante para evitar el riesgo de que el socio de negocios utilice parte del pago que le hace la organización para pagar un soborno en nombre o en beneficio de la organización. Por ejemplo, si la organización ha designado a un agente para que colabore en las ventas y se le debería pagar una comisión o un honorario contingente en el momento de la adjudicación de un contrato a la organización, la organización debería estar razonablemente convencida de que el pago de la comisión es razonable y proporcional con respecto a los servicios legítimos efectivamente prestados por el agente, teniendo en cuenta el riesgo asumido por el agente en caso de que no se adjudique el contrato. Si se paga una comisión o un honorario contingente desproporcionadamente elevado, existe un mayor riesgo de que el agente pueda utilizar indebidamente parte de la misma para inducir a un funcionario público o a un empleado del cliente de la organización a que adjudique el contrato a la organización. La organización también puede solicitar a sus socios de negocios que proporcionen documentación que demuestre que se han prestado los servicios;

c) adjudicar contratos, cuando sea posible y razonable, solo después de que se haya llevado a cabo un proceso de licitación competitivo justo y, cuando corresponda, transparente entre al menos tres competidores;

d) exigir que al menos dos personas evalúen las ofertas y aprueben la adjudicación de un contrato;

e) implementar una separación de funciones, de modo que el personal que aprueba la colocación de un contrato sea diferente de quienes solicitan la colocación del contrato y pertenezcan a un departamento o función diferente de quienes administran el contrato o aprueban el trabajo realizado bajo el contrato;

f) exigir las firmas de al menos dos personas en los contratos y en los documentos que modifican los términos de un contrato o que aprueban el trabajo realizado o los suministros proporcionados en virtud del contrato;

g) establecer un nivel más alto de supervisión de la dirección sobre las transacciones con un riesgo de soborno potencialmente alto;

h) proteger la integridad de las ofertas y otra información sensible al precio restringiendo el acceso a las personas adecuadas;

i) proporcionar herramientas y plantillas adecuadas para ayudar al personal (por ejemplo, orientación práctica, qué hacer y qué no hacer, escalas de aprobación, listas de verificación, formularios, flujos de trabajo de TI).

NOTA En la Norma ISO 37301 se proporcionan más ejemplos de controles y orientación.

A.13 Implementación del sistema de gestión antisoborno por parte de las organizaciones controladas y de los socios de negocios

A.13.1 Generalidades

A.13.1.1 La razón del requisito en el apartado 8.5 es que tanto las organizaciones controladas como los socios de negocios pueden representar un riesgo de soborno para la organización. Los tipos de riesgo de soborno que la organización pretende evitar en estos casos son, por ejemplo:

a) una filial de la organización que paga un soborno con el resultado de que la organización puede ser responsable;

b) una alianza empresarial o un socio de una alianza empresarial conjunta que paga un soborno para obtener trabajo para una alianza empresarial conjunta en la que participa la organización;

c) un gerente de compras de un cliente o comprador que exige un soborno de la organización a cambio de la adjudicación de un contrato;

d) un cliente de la organización que exige a la organización que designe a un subcontratista o proveedor específico en circunstancias en las que un gerente del cliente o un funcionario público puede beneficiarse personalmente de la designación;

e) un agente de la organización que paga un soborno a un gerente del cliente de la organización en nombre de la organización;

f) un proveedor o subcontratista de la organización que paga un soborno al gerente de compras de la organización a cambio de la adjudicación de un contrato.

A.13.1.2 Si la organización controlada o el socio de negocios ha implementado controles antisoborno en relación con esos riesgos, el riesgo de soborno consecuente para la organización normalmente se reduce.

A.13.1.3 El requisito del apartado 8.5 distingue entre aquellas organizaciones sobre las que la organización tiene control y aquellas sobre las que no lo tiene. Para los fines de este requisito, una organización tiene control sobre otra organización si controla directa o indirectamente la gestión de la organización. Una organización puede tener control, por ejemplo, sobre una subsidiaria, alianza empresarial o consorcio a través de votos mayoritarios en el directorio o a través de una participación mayoritaria en el capital. La organización no tiene control sobre otra organización a los efectos de este requisito simplemente porque le asigna una gran cantidad de trabajo.

A.13.2 Organizaciones controladas

A.13.2.1 Es razonable esperar que la organización requiera que cualquier otra organización a la que controle implemente controles antisoborno razonables y proporcionados. Esto puede hacerse mediante la implementación del mismo sistema de gestión antisoborno que la propia organización implementa, o mediante la implementación de sus propios controles antisoborno específicos. Estos controles deberían ser razonables y proporcionados en relación con los riesgos de soborno a los que se enfrenta la organización controlada, teniendo en cuenta la evaluación de riesgos de soborno realizada de conformidad con el apartado 4.5.

A.13.2.2 Cuando un socio de negocios esté controlado por la organización (por ejemplo, una alianza empresarial sobre la cual la organización tiene control de gestión), ese socio de negocios controlado estaría sujeto a los requisitos del apartado 8.5.1.

A.13.3 Socios de negocios no controlados

A.13.3.1 Con respecto a los socios de negocios que no estén controlados por la organización, es posible que la organización no necesite tomar las medidas requeridas en el apartado 8.5.2 para exigir que el socio de negocios implemente controles antisoborno en las siguientes circunstancias:

a) cuando el socio de negocios no represente un riesgo de soborno o éste sea bajo; o

b) cuando el socio de negocios represente más que un riesgo bajo de soborno, pero los controles que pueda implementar no ayudarían a mitigar el riesgo pertinente (no tendría sentido insistir en que el socio de negocios implemente controles que no ayudarían; sin embargo, en este caso, se esperaría que la organización tenga en cuenta este factor en su evaluación de riesgos para informar la decisión sobre cómo y si proceder con la relación).

A.13.3.2 Esto refleja la razonabilidad y proporcionalidad de este documento.

A.13.3.3 Si la evaluación del riesgo de soborno (véase 4.5) o la debida diligencia (véase 8.2) concluye que el socio de negocios no controlado representa más que un riesgo bajo de soborno, y que los controles antisoborno implementados por el socio de negocios ayudarían a mitigar este riesgo de soborno, la organización debería tomar las siguientes medidas adicionales según el apartado 8.5.

a) La organización determina si el socio de negocios tiene implementados controles antisoborno adecuados que gestionen el riesgo de soborno pertinente. La organización debería tomar esta determinación después de realizar la debida diligencia adecuada (véase el Capítulo A.10). La organización está tratando de verificar que estos controles gestionen el riesgo de soborno pertinente para la transacción entre la organización y el socio de negocios. La organización no necesita verificar que el socio de negocios tenga controles sobre sus riesgos de soborno más amplios. Tenga en cuenta que tanto el alcance de los controles como los pasos que la organización debería tomar para verificar estos controles deberían ser razonables y proporcionales al riesgo de soborno pertinente. Si la organización ha determinado, en la medida de lo razonablemente posible, que el socio de negocios tiene implementados controles apropiados, se aborda el requisito del apartado 8.5 en relación con ese socio de negocios.

b) Si la organización identifica que el socio de negocios no tiene implementados controles antisoborno adecuados que gestionen los riesgos de soborno pertinentes, o si no es posible verificar si tiene implementados estos controles, la organización emprende los siguientes pasos adicionales:

    1) Si es factible hacerlo, la organización requiere que el socio de negocios implemente controles antisoborno en relación con la transacción, proyecto o actividad pertinente.

    2) Cuando no sea factible exigir que el socio de negocios implemente controles antisoborno, la organización tiene este factor en cuenta al evaluar los riesgos de soborno que representa el socio de negocios y la forma en que la organización gestiona dichos riesgos. Esto no significa que la organización no pueda seguir adelante con la relación o transacción. Sin embargo, la organización

debería considerar, como parte de la evaluación del riesgo de soborno, la probabilidad de que el socio de negocios esté involucrado en un soborno, y la organización debería tener en cuenta la ausencia de tales controles al evaluar el riesgo general de soborno. Si la organización cree que los riesgos de soborno representados por este socio de negocios son inaceptablemente altos, y el riesgo de soborno no se puede reducir por otros medios (por ejemplo, reestructurando la transacción), se aplicarán las disposiciones del apartado 8.8.

A.13.3.4 El que sea o no factible para la organización exigir a un socio de negocios no controlado que implemente controles depende de las circunstancias. Por ejemplo:

a) Normalmente será factible cuando la organización tenga un grado significativo de influencia sobre el socio de negocios. Por ejemplo, cuando la organización designe a un agente para que actúe en su nombre en una transacción o designe a un subcontratista con un amplio alcance de trabajo. En este caso, la organización normalmente podrá hacer de la implementación de controles antisoborno una condición para el nombramiento.

b) Normalmente no será factible cuando la organización no tenga un grado significativo de influencia sobre el socio de negocios, por ejemplo:

   1) un cliente para un proyecto;

   2) un subcontratista o proveedor específico designado por el cliente;

   3) un subcontratista o proveedor importante cuando el poder de negociación del proveedor o subcontratista sea mucho mayor que el de la organización (por ejemplo, cuando la organización compre componentes de un proveedor importante en los términos estándar del proveedor).

c) Normalmente no será factible cuando el socio de negocios carezca de los recursos o la experiencia para poder implementar controles.

A.13.3.5 Los tipos de controles requeridos por la organización dependen de las circunstancias. Deberían ser razonables y proporcionales al riesgo de soborno, y como mínimo deberían incluir el riesgo de soborno pertinente dentro de su alcance. Dependiendo de la naturaleza del socio de negocios y la naturaleza del riesgo de soborno que representa, la organización puede, por ejemplo, tomar las siguientes medidas:

a) En el caso de un socio de negocios con alto riesgo de soborno con un alcance de trabajo amplio y complejo, la organización puede exigir que el socio de negocios haya implementado controles equivalentes a los requeridos por este documento pertinentes a los riesgos de soborno que representa para la organización.

b) En el caso de un socio de negocios de tamaño mediano y con un riesgo de soborno medio, la organización puede exigir que el socio de negocios haya implementado algunos requisitos mínimos antisoborno en relación con la transacción, por ejemplo, una política antisoborno, formación para sus empleados pertinentes, un gerente con responsabilidad por el *compliance* en relación con la transacción, controles sobre los pagos clave y una línea de reporte.

c) En el caso de socios de negocios pequeños que tienen un alcance de trabajo muy específico (por ejemplo, un agente o un proveedor menor), la organización puede exigir formación para los empleados pertinentes y controles sobre los pagos clave y los obsequios y la hospitalidad.

A.13.3.6 Los controles sólo necesitan operar en relación con la transacción entre la organización y el socio de negocios (aunque en la práctica el socio de negocios puede tener controles establecidos en relación con todo su negocio).

A.13.3.7 Los ejemplos anteriores son sólo ejemplos. Lo importante es que la organización identifique los riesgos clave de soborno en relación con la transacción y exija, en la medida de lo posible, que el socio de negocios haya implementado controles razonables y proporcionados sobre esos riesgos clave de soborno.

A.13.3.8 La organización normalmente impondrá estos requisitos al socio de negocios no controlado como condición previa para trabajar con el socio de negocios y/o como parte del documento contractual.

A.13.3.9 La organización no está obligada a verificar el cumplimiento total de estos requisitos por parte del socio de negocios no controlado. Sin embargo, la organización debería tomar medidas razonables para asegurarse de que el socio de negocios cumple (por ejemplo, solicitando al socio de negocios que proporcione copias de sus documentos de política pertinentes). En casos de alto riesgo de soborno (por ejemplo, un agente), la organización puede implementar procedimientos de seguimiento, reporte y/o auditoría.

A.13.3.10 Como la implementación de controles antisoborno puede llevar algún tiempo, es probable que sea razonable que una organización dé tiempo a sus socios de negocios para implementar dichos controles. La organización puede continuar trabajando con ese socio de negocios en el ínterin, pero la ausencia de dichos controles sería un factor en la evaluación de riesgos y la debida diligencia que se lleve a cabo. Sin embargo, la organización debería considerar exigir un derecho a rescindir el contrato o acuerdo pertinente si el socio de negocios no implementa de manera eficaz los controles requeridos de manera oportuna.

A.14 Compromisos antisoborno

A.14.1 Este requisito de obtener compromisos antisoborno solo se aplica en relación con socios de negocios que representan más que un riesgo bajo de soborno.

A.14.2 Es probable que el riesgo de soborno en relación con una transacción sea bajo, por ejemplo:

a) cuando la organización compra una pequeña cantidad de artículos de muy bajo valor;

b) cuando la organización reserva boletos de avión o habitaciones de hotel en línea directamente de las aerolíneas u hoteles;

c) cuando la organización suministra bienes o servicios de bajo valor directamente a un cliente (por ejemplo, comida, entradas de cine).

A.14.3 En estos casos, la organización no estaría obligada a obtener compromisos antisoborno de estos proveedores o clientes de bajo riesgo de soborno.

A.14.4 En el caso de un socio de negocios que represente más que un riesgo bajo de soborno, la organización debería, cuando sea posible, obtener compromisos antisoborno de ese socio de negocios.

a) Normalmente será factible exigir estos compromisos cuando la organización tenga influencia sobre el socio de negocios y pueda insistir en que el socio de negocios asuma estos compromisos. Es probable que la organización pueda exigir estos compromisos, por ejemplo, cuando designe a un agente para que actúe en su nombre en una transacción, o designe a un subcontratista con un amplio alcance de trabajo.

b) La organización puede no tener suficiente influencia para poder exigir estos compromisos en relación, por ejemplo, con los tratos con clientes importantes, o cuando la organización compre componentes a un proveedor importante en las condiciones estándar del proveedor. En estos casos, la ausencia de tales disposiciones no significa que el proyecto o la relación no deberían seguir adelante, pero la ausencia de tal compromiso debería considerarse un factor relevante en la evaluación del riesgo de soborno y la debida diligencia realizada según los apartados 4.5 y 8.2.

A.14.5 Estos compromisos deberían obtenerse, en la medida de lo posible, por escrito. Esto puede ser como un documento de compromiso separado o como parte de un contrato entre la organización y el socio de negocios.

A.15 Regalos, hospitalidad, donaciones y beneficios similares

A.15.1 La organización necesita tomar conciencia de que los regalos, la hospitalidad, las donaciones y otros beneficios pueden ser percibidos por un tercero (por ejemplo, un competidor de negocios, la prensa, un fiscal o un juez) como si tuvieran como finalidad un soborno, incluso si ni el que los da ni el que los recibe tenían esa intención. Un mecanismo de control útil es evitar, en la medida de lo posible, los regalos, la hospitalidad, las donaciones y otros beneficios que un tercero pueda razonablemente percibir como si tuvieran como finalidad un soborno.

A.15.2 Los beneficios a los que se hace referencia en el apartado 8.7 pueden incluir, por ejemplo:

a) regalos, entretenimiento y hospitalidad;

b) donaciones políticas o de caridad;

c) viajes de representantes de clientes o funcionarios públicos;

d) gastos de promoción;

e) patrocinio;

f) beneficios comunitarios;

g) formación;

h) afiliaciones a clubes;

i) favores personales;

j) información confidencial y privilegiada.

A.15.3 En relación con los obsequios y la hospitalidad, los procedimientos implementados por la organización pueden, por ejemplo, estar diseñados para:

a) controlar el alcance y la frecuencia de los obsequios y la hospitalidad mediante:
   1) una prohibición total de todos los obsequios y la hospitalidad;
   2) permitir los obsequios y la hospitalidad, pero limitándolos con referencia a factores tales como:
      i) un gasto máximo (que puede variar según la ubicación y el tipo de obsequio y hospitalidad);
      ii) frecuencia (los obsequios y la hospitalidad relativamente pequeños pueden acumularse hasta una gran cantidad si se repiten);
      iii) momento (por ejemplo, no durante o inmediatamente antes o después de las negociaciones de licitación);
      iv) razonabilidad (teniendo en cuenta la ubicación, el sector y la antigüedad del donante o del receptor);
      v) identidad del receptor (por ejemplo, aquellos en posición de adjudicar contratos o aprobar permisos, certificados o pagos);
      vi) reciprocidad (nadie en la organización puede recibir un obsequio o una hospitalidad por un valor superior al que se le permite dar);
      vii) el entorno legal y regulatorio (algunas ubicaciones y organizaciones pueden tener prohibiciones o controles establecidos);

b) exigir la aprobación previa de obsequios y hospitalidades por encima de un valor o una frecuencia definidos por un gerente apropiado;

c) exigir que los obsequios y la hospitalidad por encima de un valor o una frecuencia definidos se realicen abiertamente, se documenten de manera efectiva (por ejemplo, en un registro o libro de cuentas) y se supervisen.

A.15.4 En relación con las donaciones políticas o caritativas, los patrocinios, los gastos promocionales y los beneficios comunitarios, los procedimientos implementados por la organización pueden, por ejemplo, estar diseñados para:

a) prohibir los pagos que tengan la intención de influir, o que puedan percibirse razonablemente como que influyen, en una licitación u otra decisión a favor de la organización;

b) realizar la debida diligencia sobre el partido político, la organización benéfica u otro destinatario para determinar si son legítimos y no están siendo utilizados como canal para el soborno (por ejemplo, búsquedas en Internet u otras investigaciones apropiadas para determinar si los gerentes del partido político o la organización benéfica tienen una reputación de soborno o conducta delictiva similar, o están conectados con los proyectos o clientes de la organización);

c) exigir que un gerente apropiado apruebe el pago;

d) exigir la divulgación pública del pago;

e) asegurarse de que el pago esté permitido por la ley y las regulaciones aplicables;

f) evitar realizar contribuciones inmediatamente antes, durante o inmediatamente después de las negociaciones del contrato.

A.15.5 En relación con los viajes de representantes de clientes o funcionarios públicos, los procedimientos implementados por la organización pueden, por ejemplo, estar diseñados para:

a) permitir únicamente un pago que esté permitido por los procedimientos del cliente o del organismo público, y por la ley y los reglamentos aplicables;

b) permitir únicamente los viajes que sean necesarios para el correcto desempeño de las funciones del representante del cliente o del funcionario público (por ejemplo, para inspeccionar los procedimientos de calidad de la organización en su fábrica);

c) exigir que un gerente apropiado de la organización apruebe el pago;

d) exigir, si es posible, que se notifique al supervisor o empleador del funcionario público o a la función antisoborno sobre el viaje y la hospitalidad que se proporcionarán;

e) restringir los pagos a los gastos necesarios de viaje, alojamiento y comidas directamente asociados con un itinerario de viaje razonable;

f) limitar el entretenimiento asociado a un nivel razonable según la política de obsequios y hospitalidad de la organización;

g) prohibir el pago de los gastos de familiares o amigos;

h) prohibir el pago de gastos de vacaciones o recreativos.

A.16 Auditoría interna

A.16.1 El requisito del apartado 9.2 no significa que una organización esté obligada a tener su propia función de auditoría interna separada. Requiere que la organización designe una función o persona adecuada, competente e independiente con la responsabilidad de llevar a cabo esta auditoría. Una organización puede utilizar un tercero para operar todo su programa de auditoría interna o puede contratar a un tercero para implementar ciertas partes de un programa existente.

A.16.2 La frecuencia de la auditoría depende de los requisitos de la organización. Es probable que se seleccionen algunos proyectos, contratos, procedimientos, controles y sistemas de muestra para auditoría cada año.

A.16.3 La selección de la muestra puede basarse en el riesgo, de modo que, por ejemplo, se seleccionaría un proyecto con alto riesgo de soborno para auditoría con prioridad sobre un proyecto con bajo riesgo de soborno.

A.16.4 Las auditorías normalmente necesitarán planificarse con anticipación para que las partes pertinentes tengan los documentos necesarios y el tiempo disponible. Sin embargo, en algunos casos, la organización puede encontrar útil implementar una auditoría que las partes auditadas no esperan.

A.16.5 Si una organización tiene un órgano de gobierno, este también puede dirigir la selección y frecuencia de las auditorías de la organización según lo considere necesario, con el fin de ejercer independencia y ayudar a asegurar que las auditorías estén dirigidas a las principales áreas de riesgo de soborno de la organización. El órgano de gobierno también puede exigir el acceso a todos los informes y resultados de auditoría, y que cualquier auditoría que identifique ciertos tipos de asuntos de mayor riesgo de soborno o de indicadores de riesgo de soborno se le informe cuando se haya completado la auditoría.

A.16.6 La intención de la auditoría es proporcionar una garantía razonable al órgano de gobierno y a la alta dirección de que el sistema de gestión antisoborno se ha implementado y está funcionando de manera eficaz, para ayudar a prevenir y detectar el soborno, y para proporcionar un elemento disuasorio a cualquier personal potencialmente corrupto (ya que serán conscientes que su proyecto o departamento puede ser seleccionado para la auditoría).

A.17 Información documentada

La información documentada según el apartado 7.5.1 puede incluir:

a) recepción de la política antisoborno por parte del personal;

b) la provisión de una política antisoborno a los socios de negocios que representen un riesgo de soborno superior al bajo;

c) las políticas, procedimientos y controles del sistema de gestión antisoborno;

d) los resultados de la evaluación del riesgo de soborno (véase 4.5);

e) la formación antisoborno proporcionada (véase 7.3);

f) la debida diligencia realizada (véase 8.2);

g) las medidas adoptadas para implementar el sistema de gestión antisoborno;

h) las aprobaciones y registros de obsequios, hospitalidad, donaciones y beneficios similares otorgados y recibidos (véase 8.7);

i) las acciones y los resultados de las inquietudes planteadas en relación con:

   1) cualquier debilidad del sistema de gestión antisoborno;

   2) los incidentes de intentos de soborno, de sospechas de soborno o de soborno real;

j) los resultados del seguimiento, la investigación o la auditoría realizados por la organización o terceros.

A.18 Investigación y tratamiento de casos de soborno

A.18.1 Este documento exige que la organización implemente procedimientos adecuados sobre cómo investigar y tratar cualquier asunto de soborno o violación de los controles antisoborno que se informe, detecte o sospeche razonablemente. La forma en que una organización investigue y trate un asunto en particular dependerá de las circunstancias. Cada situación es diferente y la respuesta de la organización debería ser razonable y proporcional a las circunstancias. Un informe de un asunto importante de sospecha de soborno requeriría una acción mucho más urgente, significativa y detallada que una violación menor de los controles antisoborno. Las siguientes sugerencias se brindan solo como orientación y no deberían tomarse como prescriptivas.

A.18.2 La función antisoborno debería ser preferiblemente la receptora de cualquier informe de sospecha o soborno real o violación de los controles antisoborno. Si los informes van en primera instancia a otra persona, los procedimientos de la organización deberían exigir que el informe se transmita a la función antisoborno lo antes posible. En algunos casos, la función antisoborno identificará por sí misma una sospecha o una violación.

A.18.3 El procedimiento debería determinar quién tiene la responsabilidad de decidir cómo se investiga y se trata el asunto. Por ejemplo:

a) una organización pequeña puede implementar un procedimiento según el cual la función antisoborno debería informar inmediatamente a la alta dirección sobre todos los asuntos, independientemente de su magnitud, para que esta decida cómo responder;

b) una organización más grande puede implementar un procedimiento según el cual:

   1) la función antisoborno se ocupa de los asuntos menores y envía un informe resumido de todos los asuntos menores a la alta dirección a intervalos planificados;

   2) la función antisoborno informa inmediatamente a la alta dirección sobre los asuntos importantes para que esta decida cómo responder.

A.18.4 Cuando se identifica cualquier asunto, la alta dirección o la función antisoborno (según corresponda) debería evaluar los hechos conocidos y la gravedad potencial del asunto. Si aún no tienen suficientes hechos para tomar una decisión, deberían iniciar una investigación.

A.18.5 La investigación debería ser realizada por una persona que no haya estado involucrada en el asunto. Puede ser la función antisoborno, la auditoría interna, otro gerente o un tercero apropiado. La persona que investiga debería tener la autoridad, los recursos y el acceso adecuados por parte de la alta dirección para permitir que la investigación se lleve a cabo de manera eficaz. La persona que investiga debería tener preferiblemente formación o experiencia previa en la realización de una investigación. La investigación debería establecer rápidamente los hechos y recopilar todas las pruebas necesarias, por ejemplo:

a) realizar averiguaciones para establecer los hechos;

b) reunir todos los documentos y demás evidencias pertinentes;

c) obtener evidencias testificales;

d) cuando sea posible y razonable, solicitar que los informes sobre el asunto se hagan por escrito y estén firmados por las personas que los hayan elaborado.

A.18.6 Al llevar a cabo la investigación y cualquier acción de seguimiento, la organización debería tener en cuenta los factores pertinentes, por ejemplo:

a) las leyes aplicables (puede ser necesario el asesoramiento jurídico);

b) la seguridad del personal;

c) el riesgo de difamación al hacer declaraciones;

d) la protección de las personas que realizan los informes y de otras personas implicadas o a las que se haga referencia en el informe (véase 8.9);

e) la posible responsabilidad penal, civil y administrativa, las pérdidas financieras y el daño a la reputación de la organización y de las personas implicadas;

f) cualquier obligación legal o beneficio para la organización de informar a las autoridades;

g) mantener la confidencialidad del asunto y de la investigación hasta que se hayan establecido los hechos;

h) la necesidad de que la alta dirección exija la plena cooperación del personal en la investigación.

A.18.7 Los resultados de la investigación se deberían informar a la alta dirección o a la función antisoborno, según corresponda. Si los resultados se informan a la alta dirección, también deberían ser comunicados a la función antisoborno.

A.18.8 Una vez que la organización haya completado su investigación y/o tenga suficiente información para poder tomar una decisión, la organización debería implementar acciones de seguimiento apropiadas. Dependiendo de las circunstancias y la gravedad del asunto, estas pueden incluir una o más de las siguientes:

a) terminar, retirarse o modificar la participación de la organización en un proyecto, transacción o contrato;

b) reembolsar o reclamar cualquier beneficio indebido obtenido;

c) disciplinar al personal responsable (que, dependiendo de la gravedad del asunto, puede ir desde una advertencia por una infracción menor hasta el despido por una infracción grave);

d) informar el asunto a las autoridades;

e) si se ha producido un soborno, adoptar medidas para evitar o abordar cualquier posible infracción legal derivada de ello (por ejemplo, una contabilidad falsa que puede producirse cuando un soborno se describe falsamente en las cuentas, una infracción fiscal cuando un soborno se deduce erróneamente de los ingresos, o un lavado de dinero cuando se trata de los ingresos de un delito).

A.18.9 La organización debería revisar sus procedimientos relacionados con el antisoborno para examinar si el asunto surgió debido a alguna deficiencia en sus procedimientos y, de ser así, debería tomar medidas inmediatas y apropiadas para mejorar sus procedimientos.

A.19 Seguimiento

A.19.1 El seguimiento del sistema de gestión antisoborno puede incluir, por ejemplo, las siguientes áreas:

a) eficacia de la formación;

b) eficacia de los controles, por ejemplo, mediante resultados de pruebas de muestra;

c) eficacia de la asignación de responsabilidades para cumplir los requisitos del sistema de gestión antisoborno;

d) eficacia para abordar las fallas de cumplimiento identificadas previamente;

e) casos en los que las auditorías internas no se realizan según lo programado.

A.19.2 El seguimiento del desempeño en relación con el *compliance* puede incluir, por ejemplo, las siguientes áreas:

— incumplimiento y "cuasi accidentes" (un incidente sin efecto adverso);

— casos en los que no se cumplen los requisitos antisoborno;

— casos en los que no se logran los objetivos;

— el estatus de la cultura de *compliance*.

NOTA Véase la Norma ISO 37301.

A.19.3 La organización puede realizar, a intervalos planificados, autoevaluaciones, ya sea en toda la organización o en partes de ella, para evaluar la eficacia del sistema de gestión antisoborno (véase 9.4).

A.20 Planificación e implementación de cambios

A.20.1 La adecuación y eficacia del sistema de gestión antisoborno se debería evaluar de forma continua y regular a través de varios métodos, por ejemplo, revisiones por parte de auditorías internas (véase 9.2), la dirección (véase 9.3) y la función antisoborno (véase 9.4).

A.20.2 La organización debería considerar los resultados y las salidas de dichas evaluaciones para determinar si existe la necesidad o la oportunidad de cambiar el sistema de gestión antisoborno.

A.20.3 Para ayudar a asegurar que se mantenga la integridad del sistema de gestión antisoborno y su eficacia, los cambios en los elementos individuales del sistema de gestión deberían tener en cuenta la dependencia y el impacto de dicho cambio en la eficacia del sistema de gestión en su conjunto.

A.20.4 Cuando la organización determine la necesidad de realizar cambios en el sistema de gestión antisoborno, dichos cambios deberían llevarse a cabo de manera planificada considerando lo siguiente:

a) el propósito de los cambios y sus consecuencias potenciales;

b) la integridad del sistema de gestión antisoborno;

c) la disponibilidad de recursos;

d) la asignación o reasignación de responsabilidades y autoridad;

e) la tasa, el alcance y el marco temporal de la implementación de los cambios.

A.20.5 Las mejoras del sistema de gestión antisoborno como resultado de las medidas adoptadas en reacción a cualquier no conformidad (véase 10.2) y resultantes de las mejoras continuas (véase 10.1) deberían llevarse a cabo bajo el mismo enfoque.

A.21 Funcionarios públicos

A.21.1 El término "funcionario público" (véase 3.26) se define de manera amplia en muchas leyes anticorrupción.

A.21.2 La siguiente lista no es exhaustiva y no todos los ejemplos se aplicarán en todas las jurisdicciones. Al evaluar sus riesgos de soborno, una organización debería tener en cuenta las categorías de funcionarios públicos con los que trata o puede tratar.

A.21.3 El término funcionario público puede incluir lo siguiente:

a) titulares de cargos públicos a nivel nacional, estatal/provincial o municipal, incluidos los miembros de los órganos legislativos, los titulares de cargos ejecutivos y el poder judicial;

b) funcionarios de partidos políticos;

c) candidatos a cargos públicos;

d) empleados gubernamentales, incluidos los empleados de ministerios, agencias gubernamentales, tribunales administrativos y juntas públicas;

e) funcionarios de organizaciones internacionales públicas, por ejemplo, el Banco Mundial, las Naciones Unidas, el Fondo Monetario Internacional;

f) empleados de empresas estatales, a menos que la empresa opere sobre una base comercial normal en el mercado pertinente, es decir, sobre una base que sea sustancialmente equivalente a la de una empresa privada, sin subsidios preferenciales ni otros privilegios (véase la referencia[19]).

A.21.4 En muchas jurisdicciones, los familiares y colaboradores cercanos de funcionarios públicos también se consideran funcionarios públicos a los efectos de las leyes anticorrupción.

A.22 Iniciativas antisoborno

Aunque no es un requisito de este documento, la organización puede encontrar útil participar en cualquier iniciativa antisoborno sectorial o de otro tipo que promueva o publique buenas prácticas antisoborno pertinentes para las actividades de la organización, o tener en cuenta sus recomendaciones.

Bibliografía

[1] ISO 9000, *Sistemas de gestión de la calidad — Fundamentos y vocabulario*

[2] ISO 9001, *Sistemas de gestión de la calidad — Requisitos*

[3] ISO 14001, *Sistemas de gestión ambiental — Requisitos con orientación para su uso*

[4] ISO/IEC 17000, *Evaluación de la conformidad — Vocabulario y principios generales*

[5] ISO 19011, *Directrices para la auditoría de los sistemas de gestión*

[6] ISO 22000, *Sistemas de gestión de la inocuidad de los alimentos — Requisitos para cualquier organización en la cadena alimentaria*

[7] ISO 26000, *Guía de responsabilidad social*

[8] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[9] ISO 31000, *Gestión del riesgo — Directrices*

[10] ISO 31022, *Risk management — Guidelines for the management of legal risk*

[11] ISO 37000:2021, *Gobernanza de las organizaciones — Orientación*

[12] ISO 37002, *Sistemas de gestión de la denuncia de irregularidades — Directrices*

[13] ISO/TS 37008, *Investigaciones internas de las organizaciones — Orientación*

[14] ISO 37009:—, *Conflict of interest in organizations — Guidelines*

[15] ISO 37301, *Sistemas de gestión del compliance — Requisitos con orientación para su uso*

[16] ISO/IEC Guide 2, *Standardization and related activities — General vocabulary*

[17] United Nations Convention against Corruption, New York, 2004. Available at: https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

[18] Organization for Economic Co-operation and Development, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents, Paris, 2010

[19] Organization for Economic Co-operation and Development, Good Practice Guidance on Internal Controls, Ethics, and Compliance, Paris, 2010

[20] Organization for Economic Co-operation and Development, Commentaries on the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, 21 November 1997

[21] United Nations Global Compact/Transparency International, Reporting guidance on the 10th principle against corruption, 2009

[22] International Chamber of Commerce, Transparency International, United Nations Global Compact and World Economic Forum, RESIST: Resisting Extortion and Solicitation in International Transactions, A company tool for employee training, 2010

[23] International Chamber of Commerce, Rules on Combating Corruption, Paris, 2011

[24] Transparency International, Business Principles for Countering Bribery and associated tools, Berlin, 2013

[25] Transparency International, Corruption Perceptions Index

[26] Transparency International, Bribe Payers Index

[27] World Bank, Worldwide Governance Indicators

[28] International Corporate Governance Network, ICGN Statement and Guidance on Anti-Corruption Practices, London, 2009

[29] World Economic Forum. Partnering Against Corruption Principles for Countering Bribery, An Initiative of the World Economic Forum in Partnership with Transparency International and the Basel Institute on Governance, Geneva

[30] Committee of the Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework, May 2013

ICS 03.100.02; 03.100.01; 03.100.70

Precio basado en 47 páginas

Traducción oficial

INFORMACIÓN COMPLEMENTARIA

Documento: NTE INEN-ISO 37001	**TÍTULO: SISTEMAS DE GESTIÓN ANTISOBORNO — REQUISITOS CON ORIENTACIÓN PARA SU USO (ISO 37001:2025, IDT)**	**Código ICS: 03.100.02; 03.100.01;03. 100.70**

Fecha de iniciación del estudio: 2025-07-04

Comité Interno del INEN
Fecha de iniciación:2025-07-10 Fecha de aprobación: 2025-07-10
Integrantes del Comité:

NOMBRES:	**INSTITUCIÓN REPRESENTADA:**
Diana Zapata (Presidenta del comité)	Dirección Técnica de Reglamentación
Marcelo Arboleda	Dirección Técnica de Metrología
Ivonne Trujillo	Dirección Técnica de Validación y Certificación
Dayanna Brito	Dirección Técnica de Reglamentación
Evelyn Andrade	Dirección Técnica de Normalización
Erika Chicaiza (Secretaria Técnica de Proyectos)	Dirección Técnica de Normalización

Fechas de consulta pública: desde 2025-07-11 hasta 2025-07-26

Otros trámites: Esta NTE INEN-ISO 37001:2025 reemplaza a la NTE INEN-ISO 37001:2016 y a la NTE INEN-ISO 37001: 2016/Amd. 1:2024, IDT

La Subsecretaría de la Calidad del Ministerio de Producción, Comercio Exterior, Inversiones y Pesca aprobó este proyecto de norma.

Oficializada como: Voluntaria Por Resolución No. MPCEIP-SC-2025-0254-R de 2025-09-02
Registro Oficial No. 123, Primer Suplemento de 2025-09-12

Servicio Ecuatoriano de Normalización, INEN - Baquerizo Moreno E8-29 y Diego de Almagro
Código Postal: 170524 – Telfs.: (593 2)3 825960 al 3 825999
Centro de Información: ventanormas@normalizacion.gob.ec
URL:www.normalizacion.gob.ec