INFOSET

BASES DE ISO 37001 Y CUMPLIMIENTO ANTISOBORNO

Este curso proporciona los conocimientos esenciales para comprender y aplicar los principios de ISO 37001 y la prevención del soborno en las organizaciones.

Los participantes aprenderán a identificar riesgos de soborno, comprender controles antisoborno, aplicar principios de debida diligencia, conocer mecanismos de denuncia y fortalecer una cultura de integridad, transparencia y cumplimiento.

CURSO: BASES DE ISO 37001 Y CUMPLIMIENTO ANTISOBORNO

CONTENIDO

1. Introducción al Soborno y Marco Normativo
1.1. Definiciones y tipos de soborno
1.2. Impacto en organizaciones públicas y privadas
1.3. Ley N° 30424 (Perú)
1.4. Marco internacional: FCPA, UK Bribery Act

2. Fundamentos de la Norma ISO 37001
2.1. Origen, estructura y alcance
2.2. Ciclo PHVA aplicado al antisoborno
2.3. Términos y definiciones clave
2.4. Certificación de la organización vs. capacitación del personal
2.5. Relación con otras normas ISO

3. Liderazgo y Política Antisoborno
3.1. Rol de la alta dirección
3.2. Función de cumplimiento (oficial de cumplimiento)
3.3. Elaboración de una política antisoborno
3.4. Roles y responsabilidades

4. Evaluación de Riesgos y Debida Diligencia
4.1. Metodología de evaluación de riesgos
4.2. Debida diligencia de socios y proveedores
4.3. Riesgos en minería, construcción y contrataciones con el Estado
4.4. Gestión de regalos, hospitalidad y donaciones

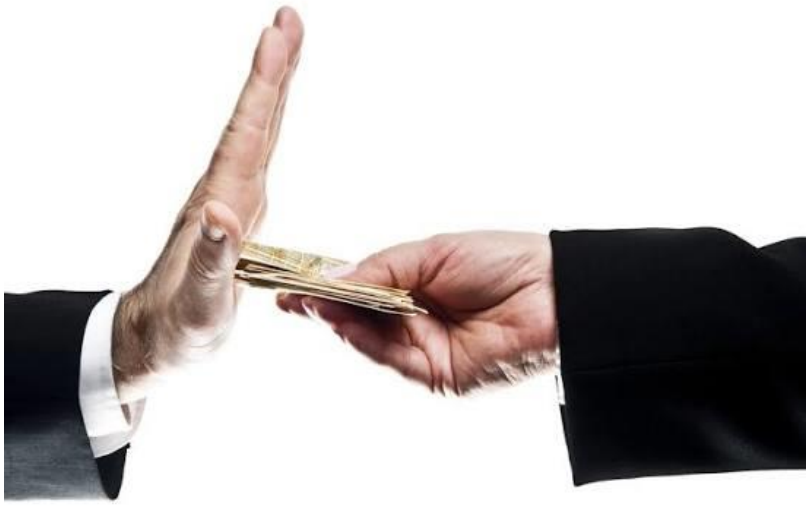
5. Controles Operativos y Financieros
5.1. Controles financieros y comerciales
5.2. Aprobación de pagos y transacciones
5.3. Canales de denuncia (whistleblowing)
5.4. Investigación de incidentes

6. Auditoría, Mejora Continua y Certificación
6.1. Auditoría interna
6.2. Revisión por la dirección
6.3. Acciones correctivas
6.4. Proceso de certificación por organismos acreditados

1. Introducción al Soborno y Marco Normativo

1.1. Definiciones y tipos de soborno

El **soborno** constituye uno de los principales riesgos de integridad y cumplimiento para las organizaciones, ya que puede afectar la toma de decisiones, distorsionar la competencia, generar pérdidas económicas y ocasionar consecuencias legales y reputacionales. La **ISO 37001:2025**, actualmente vigente, establece un marco de gestión orientado a **prevenir, detectar y responder ante situaciones de soborno**, tanto en organizaciones públicas como privadas y sin fines de lucro.



Concepto de soborno

En el contexto de la ISO 37001, el soborno comprende el **ofrecimiento, promesa, entrega, aceptación o solicitud de una ventaja indebida**, de cualquier valor, que puede ser **económica o no económica**, realizada de manera directa o indirecta y relacionada con la actuación o abstención de actuación de una persona en el ejercicio de sus funciones. La aplicación concreta de esta definición debe considerar también la legislación antisoborno que resulte aplicable a la organización.

Por lo tanto, el soborno **no se limita a la entrega de dinero en efectivo**. Una ventaja indebida puede adoptar diferentes formas, como pagos, regalos, viajes, beneficios personales, favores, oportunidades laborales, descuentos injustificados, servicios gratuitos u otros beneficios destinados a influir indebidamente en una decisión o actuación.

Un elemento fundamental es la **finalidad o intención de obtener una ventaja indebida**. Por ejemplo, ofrecer un beneficio a una persona para que favorezca a determinado proveedor, acelere indebidamente un trámite, omita un control, facilite la obtención de un contrato o adopte una decisión contraria a sus obligaciones puede constituir una situación de soborno.

Soborno activo y soborno pasivo

El soborno puede presentarse desde diferentes posiciones dentro de una relación. La ISO 37001 contempla tanto el **soborno realizado por la organización o en su nombre** como el **soborno dirigido hacia la organización, su personal o sus socios de negocio**.

El **soborno activo** se produce cuando una persona u organización **ofrece, promete o entrega una ventaja indebida** con el propósito de influir en una actuación. Por ejemplo, una empresa que ofrece dinero a un funcionario para obtener una autorización de manera indebida estaría participando en un acto de soborno activo.

El **soborno pasivo** se relaciona con la **solicitud o aceptación de una ventaja indebida**. Por ejemplo, un trabajador que solicita un beneficio personal a cambio de favorecer a un proveedor estaría frente a una situación de soborno pasivo.

Ambas situaciones representan riesgos que deben ser identificados y gestionados mediante políticas, controles y procedimientos adecuados.

Soborno directo e indirecto

El soborno puede realizarse **directamente** entre las personas involucradas o **indirectamente mediante terceros**. La ISO 37001 reconoce expresamente ambas modalidades, incluyendo situaciones en las que intervienen socios de negocio u otras personas que actúan en nombre de la organización o para su beneficio.

En un **soborno directo**, quien busca obtener una ventaja indebida se comunica o actúa directamente con la persona que tiene capacidad para tomar o influir en una decisión.

En un **soborno indirecto**, se utiliza a un tercero para realizar, facilitar o encubrir la conducta. Este tercero puede ser, dependiendo del caso, un representante, agente, consultor, intermediario, proveedor, contratista o socio de negocio.

Por esta razón, la gestión antisoborno no debe concentrarse únicamente en los trabajadores de la organización. También es necesario considerar los riesgos asociados con **terceros que actúan en nombre de la organización o mantienen relaciones comerciales con ella**.

Soborno en el sector público

En el **sector público**, el riesgo de soborno puede aparecer en actividades relacionadas con contrataciones, autorizaciones, licencias, inspecciones, fiscalización, permisos, trámites administrativos y otras decisiones en las que exista capacidad de influencia sobre recursos o decisiones públicas.

Un ejemplo sería ofrecer una ventaja indebida a un funcionario para obtener un contrato, acelerar un procedimiento que debería seguir un orden establecido, evitar una sanción o recibir un trato preferencial.

La existencia de una relación con un funcionario público **no significa por sí misma que exista soborno**. Para analizar una situación debe evaluarse la naturaleza del beneficio, las circunstancias, la finalidad de la conducta, las obligaciones de las personas involucradas y la legislación aplicable.

Soborno en el sector privado

El soborno también puede producirse dentro de relaciones entre **empresas privadas**, sin que necesariamente intervenga un funcionario público.

Por ejemplo, un trabajador encargado de seleccionar proveedores podría recibir un beneficio personal de una empresa para favorecer su contratación, alterar criterios de evaluación, proporcionar información reservada o ignorar deficiencias en una prestación.

Este tipo de situaciones demuestra que el cumplimiento antisoborno **no es exclusivamente un asunto relacionado con el Estado**. La ISO 37001 contempla expresamente los riesgos de soborno tanto en el sector público como en el privado.

Ventajas económicas y no económicas

Una ventaja indebida puede tener **valor económico o no económico**. La definición utilizada por ISO 37001 no limita el concepto de soborno a una cantidad determinada de dinero.

Entre las posibles ventajas pueden encontrarse:

- Dinero en efectivo o transferencias.
- Regalos de valor significativo.
- Viajes, alojamiento o entretenimiento.
- Pagos de gastos personales.
- Contratación de familiares o personas relacionadas.
- Ofertas de empleo o beneficios profesionales.
- Servicios gratuitos o descuentos injustificados.
- Favores personales.
- Oportunidades comerciales concedidas de manera indebida.
- Información confidencial obtenida o entregada para favorecer una decisión.

La evaluación de cada situación debe considerar **su contexto, finalidad, proporcionalidad, las políticas internas y la legislación aplicable**.

Soborno y corrupción: conceptos relacionados pero diferentes

Es importante distinguir entre **soborno** y **corrupción**. El soborno es una forma específica de conducta corrupta, mientras que la corrupción constituye un concepto más amplio que puede comprender otras conductas ilícitas o indebidas, como el abuso de funciones, el tráfico de influencias, la malversación o el enriquecimiento ilícito, dependiendo del marco jurídico aplicable.

La ISO 37001 está específicamente orientada a la **gestión del riesgo de soborno**. Una organización puede ampliar voluntariamente su sistema de gestión para abordar otros

riesgos de corrupción, pero estos no forman parte automáticamente del alcance específico de la norma.

Situaciones que requieren especial atención

En la gestión antisoborno existen determinadas situaciones que pueden presentar un riesgo elevado cuando se utilizan para influir indebidamente en una decisión. Entre ellas se encuentran los **regalos, hospitalidad, viajes, donaciones, patrocinios, contribuciones, pagos realizados mediante terceros y relaciones con proveedores o intermediarios**.

No todo regalo, atención comercial o invitación constituye automáticamente un soborno. Sin embargo, cuando existe una **ventaja indebida vinculada con la intención de influir en una decisión o actuación**, la situación debe ser evaluada y gestionada de acuerdo con los controles establecidos por la organización.

Importancia de reconocer el soborno

Identificar correctamente las diferentes formas de soborno permite a la organización establecer **controles proporcionales al nivel de riesgo**, capacitar a su personal y establecer mecanismos adecuados para prevenir, detectar y responder ante posibles incidentes.

La ISO 37001:2025 promueve un enfoque sistemático que incluye, entre otros elementos, **políticas antisoborno, evaluación de riesgos, debida diligencia, controles financieros y no financieros, capacitación, mecanismos de denuncia, seguimiento y mejora continua**.

En consecuencia, comprender qué constituye soborno y reconocer sus diferentes modalidades constituye una **base fundamental para desarrollar una cultura de integridad y cumplimiento dentro de cualquier organización**.

1.2. Impacto en organizaciones públicas y privadas

El soborno representa un **riesgo significativo para la integridad, la transparencia y la sostenibilidad de las organizaciones**, independientemente de que pertenezcan al sector público o privado. Sus efectos no se limitan a una pérdida económica inmediata: una situación de soborno puede afectar la reputación institucional, generar conflictos de interés, alterar procesos de contratación, debilitar los controles internos y producir consecuencias administrativas, civiles o penales según la naturaleza de los hechos y la legislación aplicable.

La **ISO 37001:2025** establece un marco para que las organizaciones puedan implementar, mantener y mejorar un **Sistema de Gestión Antisoborno**, orientado a prevenir, detectar y responder ante riesgos y posibles actos de soborno. La norma puede aplicarse a organizaciones de diferentes sectores y tamaños, incluidas entidades públicas, empresas privadas y organizaciones sin fines de lucro.

Impacto en las organizaciones públicas

En las entidades públicas, el riesgo de soborno puede estar relacionado con las decisiones que involucran **recursos públicos, contrataciones, autorizaciones, permisos, licencias, fiscalización, inspecciones, concesiones y prestación de servicios a los ciudadanos**.

Una conducta indebida puede producirse cuando una persona ofrece, promete o entrega una ventaja para influir en la actuación de un funcionario o servidor público. También puede presentarse cuando una persona que ocupa una posición dentro de la entidad solicita o acepta una ventaja indebida a cambio de utilizar sus funciones para favorecer determinados intereses.

Entre las situaciones que pueden presentar mayores riesgos se encuentran:

- **Contrataciones y adquisiciones públicas**, especialmente cuando existen procesos de selección, evaluación de proveedores o aprobación de contratos.
- **Otorgamiento de licencias, permisos y autorizaciones**, cuando una decisión administrativa puede generar un beneficio económico para una persona o empresa.
- **Fiscalización y supervisión**, cuando existe la posibilidad de modificar, retrasar u omitir una actuación de control.
- **Inspecciones y verificaciones**, especialmente cuando el resultado puede afectar la continuidad de una actividad económica.
- **Concesiones y autorizaciones de uso de recursos**, donde las decisiones institucionales pueden representar importantes beneficios económicos.
- **Gestión de pagos y valorizaciones**, cuando existe capacidad para aprobar, acelerar o modificar pagos.
- **Contratación de personal**, cuando una decisión puede estar influenciada por relaciones personales o intereses particulares.
- **Interacción con proveedores, contratistas y terceros**, especialmente cuando estos mantienen contacto frecuente con funcionarios o servidores públicos.

El impacto del soborno en el sector público es especialmente relevante porque puede comprometer **la confianza de los ciudadanos en las instituciones**. Cuando una decisión pública se encuentra influenciada por un beneficio indebido, se afecta el principio de igualdad y se puede generar una percepción de que el acceso a los servicios o decisiones del Estado depende de relaciones personales o pagos ilegítimos.

Impacto en las organizaciones privadas

El soborno también constituye un riesgo importante para las **empresas privadas**, incluso cuando no existe ninguna relación directa con funcionarios públicos.

Dentro de una empresa, por ejemplo, un trabajador podría recibir un beneficio personal de un proveedor para favorecerlo en un proceso de selección. También podría entregar información comercial reservada, aprobar productos o servicios que no cumplen con las condiciones pactadas, alterar una evaluación o recomendar la contratación de una empresa determinada a cambio de una ventaja personal.

Entre las situaciones de riesgo pueden encontrarse:

- **Selección y contratación de proveedores**.
- **Negociación de contratos comerciales**.
- **Compra de bienes y servicios**.
- **Aprobación de facturas y pagos**.
- **Contratación de agentes, representantes o intermediarios**.
- **Relaciones con clientes y socios de negocio**.
- **Regalos, invitaciones y hospitalidad empresarial**.
- **Donaciones y patrocinios**.
- **Contratación o promoción de trabajadores**.
- **Acceso a información confidencial o privilegiada**.

Por ello, una política antisoborno efectiva no debe limitarse a prohibir los pagos en efectivo. Debe considerar **las diferentes formas en las que una ventaja indebida puede ofrecerse, entregarse, solicitarse o aceptarse**.

Impacto económico

El soborno puede generar **costos directos e indirectos** para una organización.

Entre los costos directos pueden encontrarse pagos indebidos, pérdidas derivadas de contratos desfavorables, sobrecostos, adquisiciones innecesarias o contratación de proveedores que no cumplen adecuadamente con sus obligaciones.

Los costos indirectos pueden ser todavía más importantes. Una organización involucrada en un caso de soborno puede tener que destinar recursos a investigaciones internas, asesoría legal, auditorías extraordinarias, medidas correctivas y fortalecimiento de controles.

Además, una organización puede perder oportunidades comerciales cuando clientes, inversionistas o socios de negocio consideran que sus controles de integridad son insuficientes.

Por esta razón, la prevención del soborno debe entenderse también como una **herramienta de protección económica y de gestión empresarial**.

Impacto reputacional

La reputación constituye uno de los activos más importantes de una organización. Un incidente de soborno puede deteriorar la confianza de **clientes, proveedores, trabajadores, inversionistas, autoridades y ciudadanos**.

El impacto reputacional puede producirse incluso antes de que una investigación haya concluido, especialmente cuando una acusación recibe amplia difusión pública. Una organización puede ser percibida como poco transparente o carente de controles adecuados.

La implementación de un sistema de gestión antisoborno contribuye a establecer **políticas, responsabilidades, controles y mecanismos de seguimiento** que permiten demostrar un compromiso estructurado con la integridad.

La ISO 37001:2025 pone además mayor énfasis en la **cultura antisoborno**, reconociendo que la existencia de procedimientos escritos no es suficiente si la organización no desarrolla comportamientos y prácticas coherentes con esos principios.

Impacto en la toma de decisiones

Uno de los principales efectos del soborno es la **distorsión de las decisiones**.

Una decisión organizacional debería basarse en criterios objetivos como precio, calidad, experiencia, capacidad técnica, cumplimiento contractual, desempeño o interés público. Cuando interviene una ventaja indebida, estos criterios pueden ser reemplazados por intereses particulares.

Por ejemplo, un proveedor podría ser seleccionado no porque sea la mejor alternativa para la organización, sino porque un trabajador recibió un beneficio personal. Del mismo modo, una decisión administrativa podría favorecer a una empresa no por el cumplimiento de los requisitos establecidos, sino por una relación indebida entre las partes.

La prevención del soborno busca precisamente reducir este tipo de situaciones mediante **controles, separación de funciones, autorizaciones, evaluación de riesgos, debida diligencia y mecanismos de supervisión**.

Impacto sobre la competencia

El soborno también puede afectar la **competencia leal**.

Cuando una empresa obtiene un contrato mediante pagos indebidos, regalos o beneficios dirigidos a influir en una decisión, puede obtener una ventaja frente a competidores que participan legítimamente en el mercado.

Esto puede provocar que las organizaciones que cumplen las reglas tengan mayores dificultades para competir, mientras que aquellas dispuestas a asumir prácticas indebidas obtienen ventajas artificiales.

A largo plazo, esta situación puede deteriorar el mercado, aumentar los costos de las operaciones y reducir los incentivos para competir mediante **calidad, innovación, eficiencia y productividad**.

Impacto en los trabajadores

El soborno también puede afectar directamente el **ambiente interno de trabajo**.

Una organización que tolera prácticas indebidas puede generar una cultura en la que los trabajadores perciban que determinadas conductas son aceptables si producen resultados económicos o comerciales.

Esto puede provocar:

- Normalización de prácticas indebidas.
- Conflictos de interés.
- Pérdida de confianza entre trabajadores y directivos.
- Temor a denunciar irregularidades.
- Falta de transparencia en la toma de decisiones.
- Deterioro de la cultura organizacional.
- Riesgo de represalias contra personas que reportan conductas sospechosas.

Por ello, la prevención del soborno requiere no solamente procedimientos, sino también **liderazgo, comunicación, capacitación y una cultura organizacional basada en la integridad**.

Impacto en socios de negocio y terceros

Una organización no opera de manera aislada. Mantiene relaciones con **proveedores, contratistas, consultores, agentes, representantes, distribuidores, socios comerciales y otros terceros**.

Estas relaciones pueden generar riesgos adicionales cuando un tercero actúa en nombre de la organización o cuando sus actividades pueden afectar significativamente sus operaciones.

Por esta razón, la gestión antisoborno debe considerar la **debida diligencia de los socios de negocio**, especialmente cuando existen factores que incrementan el nivel de riesgo.

Entre los aspectos que pueden ser evaluados se encuentran la naturaleza de la relación, el tipo de actividad desarrollada, el nivel de interacción con funcionarios públicos, la ubicación geográfica, el historial de cumplimiento y la importancia económica de la relación.

Impacto en minería y construcción

En sectores como **minería y construcción**, determinados procesos pueden presentar riesgos antisoborno especialmente relevantes debido al volumen de inversiones, la interacción con autoridades, la contratación de proveedores y contratistas, la obtención de permisos y autorizaciones y la gestión de proyectos de gran escala.

Algunos escenarios que requieren especial atención son:

- Obtención de permisos y autorizaciones.
- Contratación de empresas contratistas.
- Selección de proveedores.
- Supervisión de obras y servicios.
- Aprobación de valorizaciones.
- Inspecciones y fiscalizaciones.
- Relaciones con autoridades y funcionarios.
- Gestión de comunidades y terceros.
- Donaciones y programas sociales.
- Uso de intermediarios o representantes.

La existencia de estos riesgos **no significa que exista soborno en una determinada actividad o sector**. Significa que la organización debe identificar, evaluar y tratar aquellos riesgos que sean relevantes de acuerdo con sus propias operaciones.

Impacto en las contrataciones con el Estado

Las relaciones comerciales con entidades públicas requieren especial atención debido a la interacción entre **empresas privadas, funcionarios públicos, proveedores y contratistas**.

Una empresa que participa en contrataciones con el Estado puede estar expuesta a riesgos relacionados con la preparación de propuestas, contacto con funcionarios, presentación de documentación, evaluación de ofertas, ejecución contractual, supervisión, conformidad y pagos.

Por ello, las organizaciones que participan frecuentemente en este tipo de actividades pueden beneficiarse de un sistema estructurado que permita **identificar los puntos críticos, establecer controles y documentar las decisiones relevantes**.

Consecuencias legales y responsabilidad de las organizaciones

En el Perú, la prevención del soborno también se relaciona con la **Ley N.º 30424**, que regula la responsabilidad administrativa de las personas jurídicas en el proceso penal. Esta normativa ha sido modificada posteriormente, incluyendo cambios importantes introducidos por la **Ley N.º 31740**.

El marco peruano contempla la importancia de los **modelos de prevención de delitos**, entendidos como sistemas de medidas de vigilancia y control destinados a prevenir determinados delitos o reducir significativamente el riesgo de su comisión. El Reglamento de la Ley N.º 30424 desarrolla características y elementos relacionados con estos modelos.

La normativa peruana también contempla mecanismos relacionados con la responsabilidad de las personas jurídicas y con la evaluación de los modelos de prevención. Por ello, para las empresas que desarrollan actividades en el Perú, la gestión antisoborno debe analizarse considerando tanto **las buenas prácticas internacionales como las obligaciones y riesgos establecidos por la legislación nacional**.

ISO 37001 y el cumplimiento en el Perú

La **ISO 37001 no sustituye la legislación peruana**. Se trata de una norma internacional de sistemas de gestión que proporciona requisitos y orientación para establecer, implementar, mantener, revisar y mejorar un sistema de gestión antisoborno.

En consecuencia, una organización que implemente ISO 37001 debe identificar las **leyes, reglamentos y demás requisitos aplicables a sus actividades** y establecer mecanismos adecuados para gestionarlos.

En el contexto peruano, esto permite relacionar el sistema de gestión antisoborno con el marco establecido por la **Ley N.º 30424 y sus modificaciones**, así como con las demás normas que resulten aplicables según la actividad y características de cada organización.

Es importante comprender que **contar con una certificación ISO 37001 no significa automáticamente que una organización esté exenta de responsabilidad legal ni que cumpla de manera automática todas las disposiciones de la legislación peruana**. La certificación acredita la conformidad de un sistema de gestión con los requisitos de la norma evaluados por el organismo de certificación correspondiente.

Diferencias entre el sector público y el sector privado

Aunque los principios de prevención del soborno pueden aplicarse tanto al sector público como al privado, los **riesgos concretos y los controles necesarios pueden ser diferentes**.

En el sector público, suelen tener especial importancia la transparencia, la gestión de recursos públicos, las contrataciones, las autorizaciones, la fiscalización y la relación con los ciudadanos.

En el sector privado, pueden adquirir mayor relevancia la selección de proveedores, los intermediarios, las operaciones comerciales, los pagos, los contratos, las relaciones con clientes y los procesos internos de toma de decisiones.

Sin embargo, ambos sectores comparten elementos fundamentales:

- **Compromiso de la alta dirección.**
- **Identificación y evaluación de riesgos de soborno.**
- **Políticas y procedimientos claros.**
- **Controles financieros y no financieros.**
- **Debida diligencia.**
- **Capacitación y comunicación.**
- **Canales para reportar posibles irregularidades.**
- **Investigación y tratamiento de incidentes.**
- **Seguimiento y mejora continua.**

La importancia de una cultura antisoborno

La prevención efectiva del soborno no depende exclusivamente de documentos, controles o procedimientos. También requiere construir una **cultura organizacional en la que la integridad forme parte de la manera habitual de tomar decisiones**.

La alta dirección tiene un papel fundamental porque debe establecer el ejemplo y demostrar que los objetivos comerciales, institucionales o financieros **no justifican la utilización de prácticas indebidas**.

Una cultura antisoborno efectiva permite que los trabajadores comprendan qué conductas son aceptables, cuáles presentan riesgos y cómo deben actuar cuando se enfrentan a una situación sospechosa.

Esto implica que la capacitación no debe limitarse a explicar conceptos jurídicos. Los trabajadores deben ser capaces de **reconocer situaciones de riesgo y saber qué hacer ante ellas**.

Enfoque preventivo

El objetivo principal de un sistema de gestión antisoborno es actuar **antes de que ocurra un incidente**, aunque también debe permitir detectar, investigar y responder adecuadamente cuando se presenta una situación sospechosa.

Un enfoque preventivo comprende diferentes etapas:

- Identificar los procesos donde puede existir exposición al soborno.
- Evaluar la probabilidad y el impacto de los riesgos.
- Establecer controles proporcionales al nivel de riesgo.
- Capacitar a las personas involucradas.
- Evaluar adecuadamente a determinados terceros.
- Supervisar el funcionamiento de los controles.
- Facilitar mecanismos seguros para reportar posibles irregularidades.
- Investigar las situaciones que requieran atención.
- Aplicar acciones correctivas y mejorar continuamente el sistema.

De esta manera, la gestión antisoborno deja de ser únicamente una reacción ante problemas y se convierte en **parte integral de la gestión y gobierno de la organización**.

Importancia para la sostenibilidad de la organización

Una organización que gestiona adecuadamente sus riesgos de soborno puede fortalecer su **gobernanza, transparencia, confianza y capacidad para establecer relaciones comerciales sostenibles**.

La prevención también puede contribuir a mejorar los procesos internos, clarificar responsabilidades, fortalecer los controles financieros y no financieros y establecer criterios más objetivos para la toma de decisiones.

En el contexto actual, la integridad y el cumplimiento constituyen elementos cada vez más importantes para las organizaciones que desean mantener relaciones estables con **clientes, proveedores, inversionistas, entidades públicas y otros socios de negocio**.

Por ello, la gestión antisoborno debe entenderse como una responsabilidad que involucra a **la alta dirección, la función de cumplimiento y a todos los trabajadores y personas que actúan en nombre de la organización**. Un sistema eficaz requiere compromiso continuo, evaluación de riesgos y capacidad para mejorar frente a los cambios del entorno.

La aplicación de estos principios permite que la organización avance desde una visión basada únicamente en la reacción ante casos de corrupción hacia un modelo de **prevención, control, integridad y mejora continua**, alineado con los principios de la ISO 37001:2025 y con el marco legal que resulte aplicable en el Perú.

1.3. Ley N.º 30424 (Perú)

Introducción a la Ley N.º 30424

La **Ley N.º 30424** constituye uno de los principales componentes del marco jurídico peruano relacionado con la prevención de delitos cometidos en el ámbito empresarial. Su denominación actual es **"Ley que regula la responsabilidad administrativa de las personas jurídicas en el proceso penal"**.

La norma fue publicada originalmente en 2016 y posteriormente ha sido modificada de manera importante, entre otras normas, por el **Decreto Legislativo N.º 1352, la Ley N.º 30835 y la Ley N.º 31740**. Por ello, para efectos de capacitación es importante estudiar la Ley N.º 30424 en su **versión vigente y considerando sus modificaciones**, y no únicamente el texto original.

La Ley N.º 31740, publicada en mayo de 2023, amplió significativamente el ámbito de aplicación de la Ley N.º 30424 y modificó diversas disposiciones relacionadas con la responsabilidad de las personas jurídicas, el modelo de prevención y las medidas administrativas aplicables.

Finalidad de la Ley N.º 30424

La finalidad principal de la Ley es establecer un régimen de **responsabilidad administrativa de las personas jurídicas dentro del proceso penal** por determinados delitos expresamente señalados por la legislación.

La norma busca generar incentivos para que las organizaciones adopten mecanismos internos destinados a **prevenir, identificar y mitigar riesgos de comisión de delitos** a través de sus estructuras organizacionales.

Este enfoque resulta especialmente relevante para el cumplimiento antisoborno, porque una organización no debe limitarse a reaccionar después de que ocurra un hecho ilícito. Debe establecer previamente **políticas, procedimientos, controles y mecanismos de supervisión** adecuados a sus riesgos.

La Ley N.º 30424 se complementa con su Reglamento, aprobado inicialmente mediante el **Decreto Supremo N.º 002-2019-JUS**. Este Reglamento desarrolla los componentes, estándares y requisitos relacionados con los modelos de prevención. En 2025, el Reglamento fue modificado mediante el **Decreto Supremo N.º 002-2025-JUS**, con el objetivo de adecuarlo a las modificaciones introducidas por la Ley N.º 31740.

¿A quiénes se aplica?

La Ley contempla a **personas jurídicas nacionales y extranjeras** dentro de los supuestos establecidos por la propia norma.

En el caso de las personas jurídicas extranjeras, el marco legal considera también aquellas que desarrollen actividades en el territorio peruano mediante las modalidades previstas por la legislación.

Esto significa que el cumplimiento no debe analizarse únicamente desde la perspectiva de empresas constituidas en el Perú. Una organización extranjera que desarrolla actividades en el país también debe evaluar si se encuentra dentro del ámbito de aplicación de la normativa peruana y cuáles son sus obligaciones y riesgos específicos.

Delitos comprendidos por la Ley

Uno de los cambios más importantes introducidos por la **Ley N.º 31740** fue la ampliación del catálogo de delitos que pueden generar responsabilidad de las personas jurídicas bajo la Ley N.º 30424.

Actualmente, el artículo 1 comprende determinados delitos previstos en distintas normas del ordenamiento peruano.

Entre ellos se encuentran determinados delitos del **Código Penal**, como:

- **Contabilidad paralela**, prevista en el artículo 199.
- **Atentados contra monumentos arqueológicos y zonas paleontológicas**, previstos en el artículo 226.
- **Extracción ilegal de bienes culturales y del patrimonio paleontológico**, prevista en el artículo 228.
- **Colusión simple y agravada**, prevista en el artículo 384.
- **Cohecho activo genérico**, previsto en el artículo 397.
- **Cohecho activo transnacional**, previsto en el artículo 397-A.
- **Cohecho activo específico**, previsto en el artículo 398.
- **Tráfico de influencias**, previsto en el artículo 400.

La Ley también comprende determinados delitos previstos en otras normas, incluyendo delitos relacionados con **lavado de activos, minería ilegal y crimen organizado**, delitos aduaneros, delitos tributarios y determinadas modalidades de terrorismo.

Por esta razón, el alcance actual de la Ley N.º 30424 es considerablemente más amplio que el de su versión original.

La relación entre la Ley N.º 30424 y el soborno

Para este curso resulta especialmente importante comprender la relación entre la Ley N.º 30424 y la **gestión antisoborno**.

La norma incluye dentro de su ámbito determinados delitos relacionados directamente con conductas de corrupción, entre ellos el **cohecho activo genérico, el cohecho activo transnacional, el cohecho activo específico, la colusión y el tráfico de influencias**.

Por ello, una organización que desarrolla actividades en el Perú debe considerar los riesgos relacionados con estas conductas dentro de su sistema de cumplimiento, especialmente cuando sus operaciones implican contacto con **funcionarios públicos, entidades estatales, contratistas, proveedores, intermediarios o socios comerciales**.

La gestión antisoborno basada en ISO 37001 puede constituir una herramienta importante para organizar estos controles, pero debe entenderse que **ISO 37001 y la Ley N.º 30424 son instrumentos jurídicos y de gestión diferentes**.

Responsabilidad de la persona jurídica

La Ley N.º 30424 establece supuestos en los que una persona jurídica puede ser responsable por determinados delitos cuando estos se cometen **en su nombre o por cuenta de ella y en su beneficio directo o indirecto**, bajo las condiciones establecidas por la propia legislación.

La norma contempla situaciones relacionadas con actuaciones de **socios, directores, administradores, representantes legales, apoderados y otras personas que actúen dentro de la organización**, así como determinados supuestos relacionados con trabajadores y personas sometidas a supervisión o control.

La responsabilidad de la organización no debe entenderse simplemente como una consecuencia automática de cualquier delito cometido por un trabajador. La aplicación de la Ley depende de que se cumplan los **supuestos legales establecidos para atribuir responsabilidad a la persona jurídica**.

Asimismo, la normativa establece que las personas jurídicas no son responsables cuando determinadas personas hayan cometido los delitos exclusivamente en **beneficio propio o en favor de un tercero distinto de la persona jurídica**, conforme a las condiciones previstas por la Ley.

La importancia del beneficio directo o indirecto

El concepto de **beneficio directo o indirecto** es especialmente importante para comprender la aplicación de la Ley.

Una organización puede obtener un beneficio directamente, por ejemplo, mediante la obtención de un contrato, autorización o ventaja económica.

También puede existir un beneficio indirecto cuando una conducta ilícita permite mejorar la posición comercial de la organización, facilitar una operación, evitar un perjuicio económico o generar otra ventaja para la empresa.

Sin embargo, la existencia de un beneficio por sí sola no significa automáticamente que la persona jurídica sea responsable. Deben analizarse **todos los elementos establecidos por la Ley y las circunstancias concretas del caso**.

El Modelo de Prevención de Delitos

Uno de los conceptos fundamentales de la Ley N.º 30424 es el **Modelo de Prevención de Delitos**.

Se trata de un conjunto organizado de medidas de vigilancia y control que una persona jurídica puede implementar para **prevenir, identificar y mitigar los riesgos de comisión de los delitos comprendidos por la Ley**.

La Ley establece que la persona jurídica debe elaborar su modelo de prevención considerando su **perfil de riesgo**, incluyendo los riesgos inherentes y residuales, así como el tamaño, naturaleza, características y complejidad de sus operaciones.

Esto significa que el modelo no debe ser necesariamente idéntico para todas las organizaciones.

Una empresa minera de gran tamaño, una empresa constructora, una compañía de servicios profesionales y una pequeña empresa comercial pueden tener **perfiles de riesgo diferentes** y, por lo tanto, necesitar controles diferentes.

Elementos mínimos del Modelo de Prevención

La Ley N.º 30424 establece cinco elementos mínimos para el Modelo de Prevención:

- **Encargado de prevención**, designado por el máximo órgano de administración y con autonomía para ejercer sus funciones. En las micro, pequeñas y medianas empresas, el rol puede ser asumido directamente por el órgano de administración.
- **Acciones de mitigación de los riesgos identificados**.
- **Procedimientos de denuncia**.
- **Difusión y capacitación periódica del modelo de prevención**.
- **Evaluación y monitoreo continuo del modelo**.

Estos elementos presentan una relación evidente con los principios de un sistema de gestión antisoborno.

Por ejemplo, la identificación y mitigación de riesgos se relaciona directamente con la **evaluación de riesgos antisoborno**; los procedimientos de denuncia se relacionan con los **canales de reporte**; y la capacitación y el monitoreo forman parte de la **mejora y mantenimiento del sistema**.

El encargado de prevención

El **encargado de prevención** desempeña una función fundamental dentro del Modelo de Prevención.

Debe ser designado por el máximo órgano de administración de la persona jurídica y ejercer sus funciones con **autonomía**, de acuerdo con las condiciones establecidas por la normativa.

Su función no consiste únicamente en recibir denuncias. El encargado participa en la supervisión y funcionamiento del modelo, en la identificación de riesgos, en el seguimiento de controles y en otras actividades relacionadas con la prevención.

En las micro, pequeñas y medianas empresas, la legislación permite que esta función sea asumida directamente por el órgano de administración, considerando las características y dimensión de la organización.

Identificación y mitigación de riesgos

La normativa peruana adopta un enfoque basado en riesgos. Esto significa que la organización debe identificar aquellos procesos y actividades en los que exista una exposición relevante a los delitos comprendidos por la Ley.

Entre los factores que pueden incrementar el riesgo se encuentran:

- Interacción frecuente con funcionarios públicos.
- Participación en contrataciones públicas.
- Uso de intermediarios o representantes.
- Operaciones con proveedores y contratistas.
- Actividades desarrolladas en sectores de mayor exposición.
- Operaciones internacionales.
- Manejo de grandes cantidades de recursos.
- Procesos de autorización y obtención de permisos.
- Relaciones comerciales complejas.
- Falta de controles internos adecuados.

La evaluación debe permitir determinar **qué riesgos son inherentes a la actividad y qué riesgos permanecen después de aplicar los controles existentes**. Esta distinción entre riesgo inherente y riesgo residual ha sido incorporada expresamente en el desarrollo reglamentario actualizado.

Procedimientos de denuncia

La Ley también contempla la implementación de **procedimientos de denuncia**.

Estos mecanismos permiten que las personas puedan reportar posibles delitos, intentos, sospechas o incumplimientos relacionados con el modelo de prevención.

Los canales pueden adoptar diferentes formas dependiendo de las características de la organización. Pueden incluir sistemas electrónicos, correo especializado, líneas telefónicas u otros mecanismos adecuados.

Un sistema de denuncias eficaz debe considerar aspectos como la **recepción, evaluación, investigación y tratamiento de los reportes**, así como mecanismos adecuados de protección para las personas que realizan denuncias de buena fe.

Para una organización que implementa ISO 37001, estos mecanismos pueden integrarse con el **canal de denuncias antisoborno**, siempre que se establezcan adecuadamente su alcance, responsabilidades y procedimientos.

Capacitación y difusión

La capacitación constituye uno de los elementos mínimos del Modelo de Prevención.

No es suficiente con aprobar una política o elaborar un documento interno. Los trabajadores y las personas relevantes dentro de la organización deben **conocer las reglas aplicables, reconocer situaciones de riesgo y comprender cómo actuar ante posibles irregularidades**.

La capacitación debe adaptarse al nivel de responsabilidad y exposición al riesgo de las personas.

Por ejemplo, un trabajador que realiza funciones administrativas puede enfrentar riesgos diferentes a los de un gerente encargado de negociar contratos, un comprador que selecciona proveedores o un representante que mantiene relaciones con funcionarios públicos.

Evaluación y monitoreo continuo

El Modelo de Prevención debe ser objeto de **evaluación y monitoreo continuo**.

Esto es importante porque los riesgos de una organización pueden cambiar con el tiempo. Una empresa puede ingresar a nuevos mercados, contratar nuevos intermediarios, iniciar proyectos de mayor tamaño, modificar sus procesos internos o comenzar a participar en contrataciones públicas.

Por esta razón, un modelo que fue adecuado en un determinado momento puede requerir modificaciones posteriores.

El monitoreo permite identificar **debilidades, incumplimientos y oportunidades de mejora**, mientras que la evaluación permite determinar si los controles continúan siendo adecuados frente al perfil de riesgo actual.

Modelo de Prevención e ISO 37001

La existencia de un Modelo de Prevención conforme a la Ley N.º 30424 y la implementación de un **Sistema de Gestión Antisoborno ISO 37001** no son exactamente lo mismo.

La Ley N.º 30424 establece un **marco jurídico peruano** y determina elementos mínimos para el Modelo de Prevención.

Por su parte, ISO 37001 establece requisitos para un **sistema de gestión antisoborno**, incluyendo elementos relacionados con liderazgo, política antisoborno, evaluación de riesgos, debida diligencia, controles, capacitación, comunicación, investigación, auditoría y mejora continua.

Existe una importante **complementariedad** entre ambos enfoques. Una organización puede utilizar ISO 37001 como referencia para estructurar y fortalecer sus mecanismos de prevención, siempre realizando el análisis correspondiente respecto de las exigencias específicas de la legislación peruana.

Por ello, una organización no debería asumir que **tener un certificado ISO 37001 equivale automáticamente a cumplir todas las exigencias de la Ley N.º 30424**. Son marcos distintos que deben analizarse de manera coordinada.

Evaluación del Modelo de Prevención por la SMV

La **Superintendencia del Mercado de Valores (SMV)** tiene un papel específico dentro del régimen establecido por la Ley N.º 30424.

Cuando una persona jurídica investigada alega contar con un Modelo de Prevención, la legislación contempla la emisión de un **informe técnico de la SMV** respecto de su implementación y funcionamiento, en los términos establecidos por la Ley.

El informe analiza aspectos relacionados con el modelo y tiene la condición de **pericia institucional**. La SMV puede requerir información y documentación y realizar visitas de evaluación para verificar aspectos relacionados con la implementación y funcionamiento del modelo.

Este aspecto es particularmente importante porque demuestra que un Modelo de Prevención no debe existir únicamente como un conjunto de documentos. Debe poder demostrarse que **fue implementado y que funciona efectivamente en la organización**.

Consecuencias para la persona jurídica

La Ley N.º 30424 establece diversas **medidas administrativas** que pueden ser impuestas a las personas jurídicas declaradas responsables, según las circunstancias y criterios establecidos por la legislación.

Entre ellas se encuentran:

- **Multa**.
- **Suspensión de actividades**.
- **Prohibición de realizar determinadas actividades**.
- **Prohibición definitiva de contratar con el Estado**.
- **Cancelación de licencias, concesiones, derechos y autorizaciones administrativas o municipales**.
- **Clausura de locales o establecimientos**.
- **Disolución de la persona jurídica**.

La existencia de estas medidas demuestra que el riesgo de incumplimiento antisoborno no debe considerarse únicamente como un problema reputacional. Puede convertirse también en un **riesgo jurídico, operativo, financiero y estratégico** para la organización.

La importancia de implementar el modelo antes de un incidente

Uno de los aspectos más importantes del sistema de prevención es el momento en que se implementan los controles.

La Ley contempla consecuencias específicas relacionadas con la adopción e implementación de un Modelo de Prevención y establece reglas respecto de su eficacia en función del momento en que se implementa y de las circunstancias del caso.

Por ello, una organización no debería esperar a enfrentar una investigación para comenzar a desarrollar su sistema de cumplimiento.

El verdadero objetivo de un modelo de prevención es que la organización pueda demostrar que, **antes de que ocurra un incidente**, contaba con medidas razonables y adecuadas a sus riesgos para prevenir, detectar y responder ante conductas ilícitas.

Importancia de la Ley N.º 31740

Para estudiar actualmente la Ley N.º 30424 es indispensable considerar la **Ley N.º 31740**, porque esta modificó aspectos fundamentales del régimen.

La Ley N.º 31740 amplió el catálogo de delitos, modificó disposiciones sobre responsabilidad de las personas jurídicas y actualizó las reglas relacionadas con los modelos de prevención. Además, fortaleció el enfoque relacionado con la **prevención y el buen gobierno corporativo**.

Las modificaciones introducidas por esta ley fueron posteriormente desarrolladas mediante cambios al Reglamento de la Ley N.º 30424.

En febrero de 2025 se publicó el **Decreto Supremo N.º 002-2025-JUS**, que modificó e incorporó disposiciones al Reglamento aprobado por el Decreto Supremo N.º 002-2019-JUS para adecuarlo a la Ley N.º 31740.

Por tanto, al hablar actualmente de la Ley N.º 30424, resulta necesario considerar **la Ley N.º 30424 y sus modificatorias, su Reglamento y las modificaciones reglamentarias vigentes**.

Aplicación práctica para las empresas peruanas

Para una empresa que opera en el Perú, la Ley N.º 30424 debe analizarse desde una perspectiva práctica.

La organización debe preguntarse, entre otros aspectos:

- ¿Qué delitos comprendidos en la Ley pueden afectar nuestras operaciones?
- ¿Dónde existen riesgos de soborno, colusión o tráfico de influencias?
- ¿Qué procesos presentan mayor exposición?
- ¿Qué trabajadores tienen contacto con funcionarios públicos?
- ¿Qué proveedores, agentes o intermediarios representan un riesgo elevado?

- ¿Qué controles financieros y no financieros existen?
- ¿Cómo se reciben y gestionan las denuncias?
- ¿Quién tiene la responsabilidad de supervisar el modelo?
- ¿Qué capacitación reciben los trabajadores?
- ¿Cómo se demuestra que los controles funcionan?
- ¿Con qué frecuencia se revisan y actualizan los riesgos?
- ¿Qué documentación permite demostrar la implementación y funcionamiento del modelo?

Este enfoque permite transformar la normativa en **acciones concretas de prevención y control**.

Importancia para minería, construcción y contratación pública

La Ley N.º 30424 adquiere especial relevancia para organizaciones que desarrollan actividades en sectores con una elevada interacción con autoridades, contratistas y proveedores.

En **minería y construcción**, por ejemplo, pueden existir procesos relacionados con permisos, autorizaciones, contratación de servicios, adquisición de bienes, supervisión de proyectos, valorizaciones, fiscalización y relaciones con diferentes entidades públicas.

En las **contrataciones con el Estado**, la organización debe prestar especial atención a los procesos en los que existan interacciones con funcionarios, preparación y presentación de propuestas, ejecución contractual, conformidad de servicios, valorizaciones y pagos.

La existencia de estos riesgos no implica que todas las organizaciones de estos sectores se encuentren en situación de incumplimiento. Significa que deben realizar una **evaluación específica de sus riesgos** y establecer controles proporcionales a sus operaciones.

La Ley N.º 30424 como parte de una cultura de cumplimiento

La importancia de la Ley N.º 30424 no se encuentra únicamente en las posibles sanciones. Su enfoque también busca promover una **cultura organizacional orientada a la prevención y al cumplimiento**.

Una organización que implementa correctamente sus mecanismos de prevención debe ser capaz de demostrar que la integridad forma parte de sus procesos de toma de decisiones y que la prevención de delitos constituye una responsabilidad de la organización y de las personas que participan en sus actividades.

En este sentido, la prevención debe integrarse en las operaciones habituales de la empresa y no funcionar como una actividad aislada del resto de la gestión.

Aspectos clave para recordar

La **Ley N.º 30424 es una norma peruana fundamental para comprender la responsabilidad de las personas jurídicas en determinados delitos** y el papel de los modelos de prevención.

Para efectos de este curso, los principales conceptos que deben retenerse son:

- La Ley regula la **responsabilidad administrativa de las personas jurídicas en el proceso penal**.
- Su alcance ha sido ampliado y modificado, especialmente por la **Ley N.º 31740**.
- La legislación comprende determinados delitos relacionados con **cohecho, colusión, tráfico de influencias, lavado de activos y otras conductas expresamente previstas**.
- Las organizaciones deben analizar sus riesgos de acuerdo con su **naturaleza, tamaño, características y complejidad**.
- El **Modelo de Prevención de Delitos** constituye una herramienta fundamental dentro del marco establecido por la Ley.
- Entre sus elementos mínimos se encuentran el **encargado de prevención, la mitigación de riesgos, los procedimientos de denuncia, la capacitación y el monitoreo continuo**.
- La implementación de controles debe ser **real y efectiva**, no únicamente documental.
- La **SMV** tiene funciones específicas relacionadas con la evaluación técnica de los modelos de prevención en los supuestos establecidos por la legislación.
- La **ISO 37001 y la Ley N.º 30424 son instrumentos diferentes**, aunque pueden complementarse en una estrategia integral de cumplimiento.
- Una organización debe mantener su sistema de prevención **actualizado y adaptado a la evolución de sus riesgos y del marco normativo peruano**.

En conclusión, conocer la Ley N.º 30424 permite comprender que el cumplimiento antisoborno en el Perú no constituye únicamente una cuestión de buenas prácticas empresariales. Forma parte de un **marco jurídico específico que exige a las organizaciones prestar atención a sus riesgos, fortalecer sus mecanismos de prevención y desarrollar una cultura efectiva de integridad y cumplimiento**. El estudio de esta norma constituye, por tanto, una base esencial para comprender posteriormente la aplicación práctica de ISO 37001 dentro de las organizaciones que operan en el Perú.

1.4. Marco internacional: FCPA, UK Bribery Act

Introducción al marco internacional antisoborno

La lucha contra el soborno no se limita a las leyes del país donde una organización tiene su sede. Las empresas que desarrollan **operaciones internacionales, trabajan con compañías extranjeras, participan en cadenas globales de suministro o mantienen relaciones con entidades vinculadas a otros países** pueden estar expuestas a diferentes marcos legales antisoborno.

Entre las normas internacionales más relevantes se encuentran la **Foreign Corrupt Practices Act (FCPA) de los Estados Unidos** y la **UK Bribery Act 2010 del Reino Unido**. Ambas normas tienen un impacto importante en el desarrollo de programas de cumplimiento y han contribuido a establecer estándares internacionales de prevención y control del soborno.

Estas normas no sustituyen a la legislación peruana. Para una organización que opera en el Perú, deben analizarse conjuntamente con el **marco jurídico peruano aplicable**, incluida la Ley N.º 30424 y sus modificatorias, cuando corresponda.

La importancia de estudiar la FCPA y la UK Bribery Act dentro de un curso sobre ISO 37001 radica en que ambas representan **referentes internacionales de gestión del riesgo**

de soborno, especialmente en materia de controles internos, debida diligencia, terceros, registros contables, capacitación y responsabilidad corporativa.

Foreign Corrupt Practices Act (FCPA)

La **Foreign Corrupt Practices Act (FCPA)** es una ley federal de los Estados Unidos promulgada en **1977**. Entre sus objetivos principales se encuentra prohibir determinadas formas de soborno de funcionarios públicos extranjeros con la finalidad de obtener o conservar negocios o conseguir una ventaja empresarial indebida.

La norma es especialmente relevante para empresas estadounidenses y determinadas entidades extranjeras que se encuentran dentro de su ámbito de aplicación. Su alcance puede extenderse a determinadas conductas realizadas fuera de los Estados Unidos, dependiendo de las personas, empresas, instrumentos utilizados y circunstancias involucradas.

La FCPA es particularmente importante porque combina dos grandes áreas:

- **Disposiciones antisoborno**, dirigidas principalmente a determinadas conductas relacionadas con funcionarios extranjeros.
- **Disposiciones contables**, que incluyen requisitos relacionados con los libros y registros y con los controles internos para determinadas empresas sujetas a la legislación estadounidense sobre valores.

Esta combinación convierte a la FCPA en una referencia importante para comprender la relación entre **prevención del soborno, controles financieros y transparencia contable**.

¿Qué busca prevenir la FCPA?

Las disposiciones antisoborno de la FCPA prohíben determinadas acciones destinadas a realizar, ofrecer o autorizar pagos u otras ventajas de valor a **funcionarios extranjeros**, cuando se realizan con una finalidad corrupta y para obtener o conservar negocios o conseguir una ventaja comercial indebida.

La conducta puede involucrar no solamente pagos realizados directamente, sino también determinadas operaciones realizadas **a través de terceros o intermediarios**.

Por ello, una organización debe prestar atención no solo a las acciones de sus propios trabajadores, sino también a las relaciones con **agentes, consultores, representantes, distribuidores, socios comerciales y otros terceros**.

El riesgo puede incrementarse cuando un tercero mantiene contacto frecuente con funcionarios públicos, recibe honorarios elevados sin una justificación adecuada, solicita pagos inusuales o presenta estructuras de contratación poco transparentes.

¿Quién puede ser considerado funcionario extranjero?

La interpretación del concepto de **foreign official** dentro de la FCPA es amplia.

Puede incluir a personas que trabajan para gobiernos extranjeros y determinadas entidades públicas o controladas por el Estado. También puede abarcar determinadas organizaciones internacionales públicas y personas que actúan en funciones oficiales.

Por ejemplo, dependiendo de las circunstancias, una persona que trabaja para una empresa controlada por un gobierno extranjero puede encontrarse dentro del concepto relevante para la aplicación de la FCPA.

Este aspecto resulta importante para las empresas internacionales porque la apariencia de una empresa privada **no necesariamente significa que sus trabajadores estén fuera del alcance del concepto de funcionario extranjero**. La estructura de propiedad y control de la entidad puede ser relevante.

Pagos y ventajas de valor

La FCPA no se limita exclusivamente a los pagos realizados en efectivo.

El concepto de **"anything of value"** permite considerar diferentes tipos de ventajas. Dependiendo de las circunstancias, pueden existir riesgos relacionados con:

- Dinero en efectivo.
- Regalos.
- Viajes.
- Entretenimiento.
- Gastos de alojamiento.
- Beneficios personales.
- Oportunidades laborales.
- Donaciones.
- Contribuciones u otros beneficios.

Lo importante es analizar **la naturaleza de la ventaja, las circunstancias y la finalidad de la conducta**.

Un regalo o una invitación comercial no constituye automáticamente una infracción de la FCPA. El análisis debe considerar, entre otros elementos, si existe una intención corrupta y una finalidad relacionada con obtener o mantener negocios o conseguir una ventaja indebida.

Terceros e intermediarios bajo la FCPA

Una de las áreas más importantes de cumplimiento es la utilización de **terceros**.

Las organizaciones pueden utilizar agentes, consultores, distribuidores o representantes para desarrollar actividades en otros países. Sin embargo, la utilización de un tercero no debe convertirse en un mecanismo para ocultar un pago indebido.

Por esta razón, las organizaciones deben aplicar procedimientos de **debida diligencia basados en el riesgo** antes y durante determinadas relaciones con terceros.

Entre las señales que pueden justificar una revisión adicional se encuentran:

- Solicitudes de honorarios desproporcionados.
- Falta de claridad sobre los servicios que serán prestados.
- Solicitud de pagos a cuentas bancarias inusuales.
- Solicitud de pagos en efectivo sin justificación.
- Relaciones personales o familiares relevantes con funcionarios.
- Historial de problemas de integridad.
- Resistencia a proporcionar información básica sobre la empresa.
- Estructuras de contratación innecesariamente complejas.
- Solicitud de pagos a través de terceros no relacionados con el servicio.

La debida diligencia de terceros constituye, por tanto, un elemento estrechamente relacionado con los principios de **ISO 37001**.

Disposiciones contables de la FCPA

Una característica especialmente importante de la FCPA es que no se concentra exclusivamente en el soborno.

Las disposiciones contables incluyen requisitos relacionados con **books and records** y **internal accounting controls** para las entidades comprendidas dentro de su ámbito.

Los libros y registros deben reflejar las transacciones y disposiciones de activos con un nivel razonable de detalle y de manera adecuada. Además, deben existir controles internos destinados a proporcionar un grado razonable de seguridad respecto de la correcta autorización y registro de las operaciones.

Esto significa que una empresa no puede intentar ocultar un pago indebido mediante una descripción falsa en sus registros contables.

Por ejemplo, registrar un pago indebido como si fuera un **servicio de consultoría**, una comisión legítima o un gasto comercial inexistente puede generar riesgos adicionales relacionados con las disposiciones contables de la FCPA.

Importancia de los controles financieros

La FCPA demuestra claramente que la prevención del soborno también depende de **controles financieros adecuados**.

Entre los controles que pueden ayudar a reducir riesgos se encuentran:

- Separación de funciones.
- Autorización previa de determinados pagos.
- Revisión de proveedores y terceros.
- Documentación de gastos.
- Conciliaciones bancarias.
- Controles sobre cuentas y registros contables.
- Supervisión de pagos extraordinarios.
- Revisión de comisiones y honorarios.

- Controles sobre regalos y hospitalidad.
- Auditorías y revisiones periódicas.

Estos principios guardan una relación directa con el módulo de **Controles Operativos y Financieros** de este curso.

UK Bribery Act 2010

La **UK Bribery Act 2010** es una de las legislaciones antisoborno más relevantes del Reino Unido.

La norma establece diferentes delitos relacionados con el soborno y presenta un alcance amplio. Entre sus características se encuentra la regulación tanto del **soborno de personas** como del **soborno de funcionarios públicos extranjeros**, así como la responsabilidad corporativa por determinadas situaciones en las que una organización comercial no evita que personas asociadas con ella realicen actos de soborno.

El Ministerio de Justicia del Reino Unido ha desarrollado una guía específica para ayudar a las organizaciones comerciales a establecer procedimientos adecuados para prevenir el soborno. Esta guía se estructura alrededor de **seis principios fundamentales**.

Principales delitos contemplados por la UK Bribery Act

La UK Bribery Act contempla, entre otros, los siguientes delitos:

- **Ofrecer, prometer o dar un soborno**.
- **Solicitar, acordar recibir o aceptar un soborno**.
- **Sobornar a un funcionario público extranjero** para obtener o conservar una ventaja comercial.
- **Fallo de una organización comercial en prevenir el soborno**, bajo las condiciones establecidas por la norma.

Esta estructura es importante porque la ley no se limita a castigar a quien entrega un soborno. También contempla la conducta de quien **solicita o acepta** una ventaja indebida.

Soborno de funcionarios públicos extranjeros

La UK Bribery Act contempla específicamente el delito de **bribery of a foreign public official**.

El objetivo es evitar que una organización o persona utilice beneficios indebidos para influir en un funcionario público extranjero con la finalidad de obtener o conservar una ventaja comercial.

Para organizaciones internacionales, esto significa que determinadas relaciones con funcionarios públicos de otros países deben ser gestionadas mediante controles adecuados.

En el caso de una empresa que opera en Perú, por ejemplo, determinadas interacciones con funcionarios peruanos podrían adquirir relevancia bajo una legislación

extranjera cuando la organización se encuentre dentro del ámbito de aplicación correspondiente.

El delito de “failure to prevent bribery”

Una de las características más conocidas de la UK Bribery Act es el delito de «**failure of commercial organisations to prevent bribery»**.

En términos generales, una organización comercial puede enfrentar responsabilidad cuando una persona asociada con ella soborna a otra persona con la intención de obtener o conservar negocios o una ventaja comercial para la organización, salvo que la organización pueda demostrar que tenía implementados **procedimientos adecuados diseñados para prevenir el soborno**.

Este enfoque tiene una gran importancia para los sistemas de cumplimiento porque desplaza parte de la atención hacia la **capacidad preventiva de la organización**.

No basta con afirmar que la dirección desconocía el comportamiento del trabajador o tercero. La organización debe poder demostrar que estableció medidas razonables y proporcionales para prevenir el riesgo.

Los seis principios de prevención del soborno en el Reino Unido

La guía oficial del Ministerio de Justicia del Reino Unido desarrolla seis principios para ayudar a las organizaciones a establecer procedimientos adecuados de prevención:

- **Proporcionalidad de los procedimientos**: las medidas deben ser proporcionales a los riesgos y a la naturaleza, escala y complejidad de la organización.
- **Compromiso de la alta dirección**: los órganos de dirección deben demostrar una cultura de integridad y tolerancia cero frente al soborno.
- **Evaluación del riesgo**: la organización debe identificar, evaluar y revisar periódicamente sus riesgos.
- **Debida diligencia**: deben aplicarse procedimientos adecuados respecto de las personas y organizaciones que puedan representar riesgos.
- **Comunicación y capacitación**: las políticas y procedimientos deben comunicarse y explicarse de manera adecuada.
- **Monitoreo y revisión**: los procedimientos deben ser revisados y mejorados cuando sea necesario.

Estos seis principios presentan una relación muy cercana con el enfoque de **ISO 37001**, especialmente en materia de liderazgo, evaluación de riesgos, debida diligencia, capacitación, controles y mejora continua.

¿Qué significa “procedimientos adecuados”?

La expresión **“adequate procedures”** no significa que exista un conjunto universal de documentos que todas las empresas deban utilizar.

Los procedimientos deben ser **proporcionales al riesgo**.

Una empresa pequeña con operaciones limitadas puede requerir controles diferentes de los de una corporación multinacional que trabaja con cientos de proveedores y mantiene operaciones en diferentes países.

La organización debe demostrar que sus medidas fueron diseñadas teniendo en cuenta sus **riesgos reales y específicos**.

Por ello, una política antisoborno genérica que no considera las características de la organización puede ser insuficiente como mecanismo de gestión del riesgo.

Diferencia entre FCPA y UK Bribery Act

Aunque ambas normas buscan combatir el soborno, existen diferencias importantes.

La **FCPA** se concentra principalmente en determinadas formas de soborno de funcionarios públicos extranjeros y, para determinadas entidades, contiene además disposiciones contables relacionadas con libros, registros y controles internos.

La **UK Bribery Act**, por su parte, tiene un alcance más amplio respecto del soborno y contempla tanto el soborno activo como el pasivo, además de un delito específico de **failure to prevent bribery** para organizaciones comerciales.

Una comparación básica puede resumirse de la siguiente manera:

Aspecto	FCPA	UK Bribery Act
País de origen	Estados Unidos	Reino Unido
Año principal	1977	2010
Soborno de funcionarios extranjeros	Sí	Sí
Soborno entre particulares	No constituye el núcleo principal de la FCPA	Sí
Soborno activo	Sí	Sí
Soborno pasivo	No constituye el núcleo de las disposiciones antisoborno	Sí
Responsabilidad por no prevenir soborno	No bajo una figura equivalente a la del UK Bribery Act	Sí, bajo determinadas condiciones
Controles contables	Sí, para entidades comprendidas en las disposiciones contables	No existe un equivalente directo dentro de la UK Bribery Act
Debida diligencia de terceros	Muy relevante	Muy relevante

Programas de cumplimiento	Muy relevantes	Muy relevantes

La comparación permite observar que ambas normas utilizan enfoques diferentes, pero coinciden en la importancia de **prevenir, detectar y responder ante los riesgos de soborno**.

Alcance internacional de estas normas

Un aspecto fundamental es comprender que una ley nacional puede tener **efectos internacionales**.

Una empresa ubicada en Perú no debe asumir automáticamente que las normas extranjeras no le afectan. La aplicabilidad de la FCPA o de la UK Bribery Act depende de factores jurídicos concretos relacionados con la organización, las personas involucradas, sus operaciones, sus vínculos corporativos y las conductas realizadas.

Por esta razón, las empresas que trabajan con **grupos empresariales internacionales, inversionistas extranjeros, clientes multinacionales, proveedores internacionales o mercados extranjeros** deben evaluar si están expuestas a requisitos adicionales.

Este análisis debe realizarse con asesoramiento jurídico especializado cuando exista una cuestión concreta de aplicabilidad.

Relación con las empresas peruanas

Para una empresa peruana, el conocimiento de la FCPA y la UK Bribery Act puede ser relevante incluso cuando su actividad principal se desarrolla dentro del país.

Por ejemplo, una empresa peruana podría formar parte de la cadena de suministro de una compañía estadounidense o británica, trabajar para un grupo empresarial internacional o participar en proyectos financiados o gestionados por organizaciones extranjeras.

En estos casos, pueden surgir **requisitos contractuales de cumplimiento**, procesos de debida diligencia, cuestionarios de integridad, obligaciones de reporte y exigencias relacionadas con programas antisoborno.

Por ello, conocer estos marcos permite a los trabajadores comprender por qué determinadas empresas exigen políticas estrictas respecto de **regalos, hospitalidad, pagos, terceros, conflictos de interés y documentación de operaciones**.

Relación con ISO 37001

La **ISO 37001** no es una legislación de los Estados Unidos ni del Reino Unido. Es un estándar internacional de sistema de gestión.

Su objetivo es proporcionar requisitos para que una organización pueda establecer un sistema estructurado para **prevenir, detectar y responder ante el soborno**.

Por esta razón, existe una relación conceptual importante entre ISO 37001 y los principales marcos antisoborno internacionales.

Algunos elementos comunes son:

- **Compromiso de la alta dirección**.
- **Política antisoborno**.
- **Evaluación de riesgos**.
- **Debida diligencia**.
- **Controles financieros y no financieros**.
- **Capacitación y comunicación**.
- **Canales de denuncia**.
- **Investigación de posibles incidentes**.
- **Monitoreo y auditoría**.
- **Acciones correctivas**.
- **Mejora continua**.

Esto permite que una organización diseñe un sistema de cumplimiento que no dependa exclusivamente de una legislación determinada, sino que tenga una estructura capaz de **adaptarse a diferentes requisitos legales y regulatorios aplicables**.

Regalos, hospitalidad y gastos comerciales

La gestión de **regalos, hospitalidad, viajes y gastos comerciales** es una de las áreas donde pueden aparecer riesgos bajo diferentes marcos antisoborno.

No debe interpretarse que cualquier regalo o invitación constituye automáticamente un soborno.

El análisis debe considerar factores como:

- Valor del beneficio.
- Frecuencia.
- Momento en que se ofrece.
- Identidad del destinatario.
- Relación comercial existente.
- Existencia de un proceso de contratación.
- Finalidad del beneficio.
- Transparencia del gasto.
- Reglas internas de la organización.
- Legislación aplicable.

Un beneficio aparentemente pequeño puede presentar un riesgo elevado si se entrega **justo antes de una decisión importante y con la intención de influir en ella**.

Por esta razón, las organizaciones deben establecer criterios claros y controles proporcionales.

Importancia de los terceros

Tanto la experiencia internacional asociada con la FCPA como la orientación del Reino Unido resaltan la importancia de gestionar los riesgos derivados de **terceros**.

Una empresa puede establecer controles estrictos para sus trabajadores, pero quedar expuesta si utiliza intermediarios sin realizar una evaluación adecuada.

Por ello, la debida diligencia puede incluir:

- Identificación del tercero.
- Verificación de su existencia y estructura.
- Identificación de propietarios o beneficiarios cuando sea relevante.
- Evaluación de antecedentes.
- Análisis de su reputación.
- Evaluación de posibles conflictos de interés.
- Revisión de la naturaleza y justificación de sus honorarios.
- Inclusión de cláusulas contractuales de cumplimiento.
- Monitoreo durante la relación comercial.

La intensidad de estos procedimientos debe ser **proporcional al nivel de riesgo**.

Importancia de los registros y la documentación

Un sistema antisoborno necesita poder demostrar qué decisiones se tomaron, quién las autorizó y qué controles fueron aplicados.

La documentación permite demostrar, por ejemplo:

- Que se realizó una evaluación de riesgos.
- Que un tercero fue sometido a debida diligencia.
- Que un pago fue revisado y autorizado.
- Que una capacitación fue realizada.
- Que una denuncia fue recibida y gestionada.
- Que un incidente fue investigado.
- Que una acción correctiva fue implementada.
- Que la dirección revisó el funcionamiento del sistema.

La documentación no debe convertirse en una carga burocrática sin finalidad. Su propósito es proporcionar **evidencia de que los controles existen y funcionan**.

Lecciones para las organizaciones

El estudio de la FCPA y de la UK Bribery Act permite identificar varias lecciones importantes para cualquier organización.

La primera es que **la prevención debe comenzar antes de que ocurra un incidente**.

La segunda es que los riesgos no se encuentran únicamente dentro de la organización. También pueden surgir a través de **terceros, proveedores, agentes, representantes y socios de negocio**.

La tercera es que los controles financieros son fundamentales para detectar pagos irregulares y evitar que una operación indebida quede oculta dentro de los registros contables.

La cuarta es que una política antisoborno debe estar respaldada por **liderazgo, capacitación, controles y mecanismos de supervisión**.

La quinta es que los procedimientos deben adaptarse al **riesgo real de la organización** y no limitarse a documentos genéricos.

Aplicación práctica en el Perú

Para una organización que opera en Perú, el conocimiento de estos marcos internacionales permite desarrollar una perspectiva más completa del cumplimiento.

La organización debe comenzar por identificar las **normas peruanas que le resultan aplicables**, incluyendo la Ley N.º 30424 y sus modificatorias cuando corresponda.

Posteriormente, debe determinar si existen obligaciones o riesgos derivados de **relaciones internacionales**.

Finalmente, puede utilizar los principios de ISO 37001 y las buenas prácticas internacionales como referencia para fortalecer su sistema de gestión.

De esta manera, el cumplimiento antisoborno puede construirse sobre tres niveles complementarios:

Legislación peruana, que establece las obligaciones jurídicas nacionales aplicables.

Marcos internacionales, como la FCPA y la UK Bribery Act, que pueden resultar relevantes dependiendo de las relaciones y operaciones de la organización.

ISO 37001, que proporciona un marco estructurado para gestionar el riesgo de soborno mediante un sistema de gestión.

Aspectos clave para recordar

La **FCPA y la UK Bribery Act son dos referentes internacionales fundamentales en materia antisoborno**, pero no son equivalentes entre sí.

La FCPA destaca especialmente por sus disposiciones sobre **soborno de funcionarios extranjeros, terceros, registros contables y controles internos**.

La UK Bribery Act presenta un alcance amplio sobre el soborno y destaca por el delito de **failure to prevent bribery**, que incentiva a las organizaciones comerciales a implementar procedimientos adecuados y proporcionales para prevenir el soborno.

Para una organización que opera en el Perú, estas normas **no sustituyen la legislación peruana** y su aplicabilidad dependerá de las circunstancias concretas.

Sin embargo, su estudio permite comprender por qué los sistemas modernos de cumplimiento prestan tanta atención a:

- **La evaluación de riesgos.**
- **El compromiso de la alta dirección.**
- **La debida diligencia de terceros.**
- **Los controles financieros.**
- **Los registros contables transparentes.**
- **La capacitación del personal.**
- **Los canales de denuncia.**
- **La investigación de incidentes.**
- **El monitoreo y la mejora continua.**

Estos elementos constituyen también componentes esenciales de una gestión antisoborno eficaz y preparan al participante para comprender los siguientes módulos del curso, especialmente aquellos relacionados con **ISO 37001, liderazgo, evaluación de riesgos, debida diligencia y controles operativos y financieros**.

2. Fundamentos de la Norma ISO 37001

2.1. Origen, estructura y alcance

Introducción a la ISO 37001

La **ISO 37001** es una norma internacional desarrollada específicamente para establecer, implementar, mantener y mejorar un **Sistema de Gestión Antisoborno (SGAS)** dentro de una organización.

Su finalidad es proporcionar un marco estructurado que permita a las organizaciones **prevenir, detectar y responder ante el soborno**, así como gestionar las obligaciones legales y otros compromisos antisoborno que resulten aplicables a sus actividades. La norma puede utilizarse en organizaciones públicas, privadas y sin fines de lucro.

Es importante señalar que la versión actualmente vigente es **ISO 37001:2025, segunda edición**, publicada el **28 de febrero de 2025**. Esta edición sustituyó a la ISO 37001:2016, que actualmente se encuentra retirada.

Por ello, cuando una organización estudia o implementa actualmente ISO 37001, debe tomar como referencia la **edición 2025** y no la versión 2016.

Origen de la norma

La ISO 37001 fue desarrollada dentro del sistema de normalización internacional de ISO como respuesta a la necesidad de disponer de un marco común para la **gestión sistemática del riesgo de soborno**.

La primera edición fue publicada en **octubre de 2016**. Durante los años siguientes, la experiencia obtenida por las organizaciones y los cambios en las prácticas internacionales de gobierno, cumplimiento e integridad llevaron a la revisión de la norma.

La segunda edición, **ISO 37001:2025**, fue publicada en febrero de 2025 después de un proceso internacional de revisión y aprobación. La edición anterior, ISO 37001:2016, fue retirada con la publicación de la nueva versión.

La actualización busca mantener la norma alineada con las prácticas actuales de gestión y con otros estándares internacionales de sistemas de gestión. Entre las novedades y aclaraciones de la edición 2025 se encuentran aspectos relacionados con **la cultura de cumplimiento, la gestión de conflictos de interés, la función antisoborno y otros elementos del sistema de gestión**.

¿Qué es un Sistema de Gestión Antisoborno?

Un **Sistema de Gestión Antisoborno (SGAS)** es un conjunto organizado de políticas, procedimientos, responsabilidades, controles y procesos mediante los cuales una organización gestiona sus riesgos relacionados con el soborno.

No se trata simplemente de elaborar una política y distribuirla entre los trabajadores.

Un sistema de gestión implica establecer una estructura que permita:

- **Identificar los riesgos de soborno**.
- Evaluar la probabilidad y el impacto de dichos riesgos.
- Establecer controles adecuados.
- Definir responsabilidades.
- Capacitar y sensibilizar al personal.
- Evaluar a determinados socios de negocio y terceros.
- Controlar determinadas operaciones financieras y comerciales.
- Recibir y gestionar denuncias.
- Investigar posibles incidentes.
- Supervisar el funcionamiento del sistema.
- Realizar auditorías y revisiones.
- Aplicar acciones correctivas.
- **Mejorar continuamente el sistema**.

La ISO 37001 establece requisitos y orientación para que estos elementos funcionen como un **sistema integrado**, y no como actividades independientes.

Objetivo principal de ISO 37001

El objetivo fundamental de la norma es ayudar a una organización a establecer mecanismos que permitan **prevenir, detectar y responder ante el soborno**.

Esto implica trabajar en tres dimensiones. La primera es la **prevención**, mediante políticas, evaluación de riesgos, debida diligencia, capacitación y controles.

La segunda es la **detección**, mediante mecanismos de supervisión, controles financieros y no financieros, canales de denuncia, auditorías y otras herramientas.

La tercera es la **respuesta**, mediante investigación de incidentes, acciones correctivas, tratamiento de incumplimientos y mejora del sistema.

Por lo tanto, ISO 37001 no pretende garantizar que una organización nunca enfrentará un intento de soborno. Su propósito es establecer un sistema que permita **reducir el riesgo y actuar adecuadamente cuando se presenta una situación de este tipo**.

¿Qué entiende ISO 37001 por soborno?

La norma aborda diferentes formas de soborno, incluyendo el **soborno directo e indirecto**.

Esto significa que el sistema debe considerar no solamente los pagos o beneficios entregados directamente por trabajadores de la organización, sino también situaciones en las que pueden intervenir **terceros, intermediarios, representantes, proveedores, contratistas o socios de negocio**.

El soborno tampoco debe entenderse exclusivamente como una entrega de dinero.

Dependiendo de las circunstancias, puede involucrar diferentes tipos de **ventajas indebidas**, por lo que la organización debe evaluar sus riesgos de acuerdo con la naturaleza de sus operaciones.

Alcance de ISO 37001

Una de las características importantes de ISO 37001 es que puede aplicarse a **organizaciones de diferentes sectores, tamaños y naturalezas**.

La norma puede utilizarse en:

- **Empresas privadas**.
- **Entidades del sector público**.
- Organizaciones sin fines de lucro.
- Empresas nacionales.
- Organizaciones con operaciones internacionales.
- Organizaciones grandes y pequeñas.

La norma no está limitada a un sector económico específico. Por ello, puede resultar aplicable a organizaciones que desarrollan actividades en **minería, construcción, industria, comercio, servicios, transporte, energía, administración pública y otros sectores**.

Aplicación en organizaciones públicas

En el sector público, un Sistema de Gestión Antisoborno puede utilizarse para gestionar riesgos relacionados con procesos como:

- Contrataciones y adquisiciones.
- Licencias y autorizaciones.
- Fiscalización e inspecciones.
- Gestión de permisos.
- Contratos y convenios.
- Administración de recursos públicos.

- Relaciones con proveedores y contratistas.
- Interacción con ciudadanos y empresas.
- Gestión de proyectos públicos.

La organización debe determinar cuáles de estos procesos son relevantes según su propio contexto y **evaluar los riesgos de soborno asociados a sus actividades**.

Aplicación en organizaciones privadas

En el sector privado, ISO 37001 puede utilizarse para gestionar riesgos relacionados con:

- Selección y contratación de proveedores.
- Compras y adquisiciones.
- Ventas y relaciones comerciales.
- Contratación de intermediarios.
- Representantes y agentes.
- Negociación de contratos.
- Pagos y operaciones financieras.
- Regalos y hospitalidad.
- Donaciones y patrocinios.
- Relaciones con funcionarios públicos.
- Participación en contrataciones estatales.

La organización debe determinar qué procesos presentan mayor exposición y establecer **controles proporcionales al nivel de riesgo**.

ISO 37001 no es una ley

Un punto fundamental para comprender la norma es que **ISO 37001 no es una ley ni un reglamento gubernamental**.

Se trata de una **norma internacional de gestión**. Esto significa que la organización utiliza sus requisitos como marco para desarrollar un sistema de gestión antisoborno. Sin embargo, debe continuar cumpliendo las leyes y regulaciones que sean aplicables a sus actividades.

En el caso de una organización que opera en Perú, por ejemplo, ISO 37001 debe analizarse conjuntamente con el **marco jurídico peruano aplicable**, incluyendo la Ley N.º 30424 y sus modificatorias cuando corresponda.

La propia ISO 37001 contempla que el sistema debe ayudar a la organización a cumplir con las **leyes antisoborno aplicables y otros compromisos voluntarios que haya asumido**.

ISO 37001 y la legislación peruana

La relación entre ISO 37001 y la legislación peruana es especialmente importante para las organizaciones que desarrollan actividades en el Perú.

La organización debe identificar las normas jurídicas que le resultan aplicables y determinar cómo serán gestionadas dentro de su sistema.

En materia de prevención de delitos y responsabilidad de las personas jurídicas, la **Ley N.º 30424 y sus modificaciones** constituye uno de los elementos relevantes del marco peruano.

Por tanto, una empresa puede utilizar ISO 37001 como una herramienta para estructurar y fortalecer su sistema antisoborno, pero debe realizar un análisis específico para determinar **qué exigencias legales peruanas le corresponden**.

Estructura general de la norma

ISO 37001:2025 sigue la estructura común utilizada por numerosas normas ISO de sistemas de gestión.

Esta estructura permite integrar el Sistema de Gestión Antisoborno con otros sistemas de gestión existentes dentro de la organización.

De manera general, el contenido se organiza alrededor de los siguientes elementos:

- **Contexto de la organización**.
- **Liderazgo**.
- **Planificación**.
- **Apoyo**.
- **Operación**.
- **Evaluación del desempeño**.
- **Mejora**.

Esta estructura facilita que la gestión antisoborno no funcione como un programa aislado, sino como parte del **sistema general de gestión de la organización**.

Contexto de la organización

El sistema comienza con la comprensión del **contexto de la organización**.

Antes de establecer controles, la organización necesita comprender qué hace, cómo opera, quiénes son sus principales partes interesadas y cuáles son las circunstancias que pueden afectar su capacidad para gestionar los riesgos de soborno.

Esto puede incluir aspectos como:

- Tamaño de la organización.
- Estructura corporativa.
- Actividades y mercados.
- Ubicación geográfica.
- Tipo de clientes.
- Relaciones con entidades públicas.
- Uso de intermediarios.
- Estructura de proveedores.

- Operaciones internacionales.
- Obligaciones legales y contractuales.

El objetivo es evitar que el sistema antisoborno sea diseñado de manera genérica y desconectada de la realidad de la organización.

Liderazgo

El **liderazgo de la alta dirección** constituye un componente esencial del sistema.

La prevención del soborno no puede depender exclusivamente del área de cumplimiento o de una persona designada como responsable.

La alta dirección debe demostrar compromiso con el sistema, establecer una política adecuada y promover una **cultura organizacional basada en la integridad**.

Los trabajadores deben percibir que la organización no tolera prácticas de soborno y que las decisiones comerciales o institucionales no justifican la utilización de medios indebidos.

Planificación y enfoque basado en riesgos

La organización debe establecer una metodología para **identificar y evaluar sus riesgos de soborno**.

El análisis debe considerar las características específicas de sus actividades.

Por ejemplo, una empresa que participa frecuentemente en contrataciones públicas puede presentar riesgos diferentes a los de una empresa que vende directamente al consumidor.

Una empresa minera puede tener riesgos relacionados con permisos, contratistas, proveedores y autoridades, mientras que una empresa de servicios profesionales puede presentar mayor exposición en sus relaciones con clientes, intermediarios y procesos comerciales.

Por ello, la evaluación debe permitir identificar **dónde, cómo y por qué podría producirse un soborno**.

Apoyo al sistema

Un sistema de gestión requiere recursos y capacidades para funcionar.

Entre los elementos de apoyo se encuentran:

- Competencia del personal.
- Capacitación.
- Comunicación.
- Información documentada.

- Recursos necesarios para operar el sistema.
- Concientización de los trabajadores.
- Definición clara de responsabilidades.

La capacitación es especialmente importante porque los trabajadores deben conocer **los riesgos que enfrentan en sus funciones y cómo actuar ante situaciones sospechosas**.

Operación

La parte operativa representa la aplicación práctica del sistema.

Aquí se encuentran diferentes mecanismos destinados a gestionar los riesgos, como:

- Debida diligencia.
- Controles financieros.
- Controles no financieros.
- Gestión de regalos y hospitalidad.
- Controles sobre determinadas operaciones.
- Gestión de terceros.
- Investigación de posibles incidentes.
- Procedimientos relacionados con denuncias.

Estos mecanismos deben estar relacionados con los riesgos identificados y funcionar de manera coherente con las políticas de la organización.

Evaluación del desempeño

Un sistema antisoborno no debe permanecer estático.

La organización debe **evaluar periódicamente si el sistema funciona como estaba previsto**.

Para ello puede utilizar herramientas como:

- Indicadores.
- Seguimiento de controles.
- Auditorías internas.
- Revisiones de la dirección.
- Evaluaciones de riesgos.
- Análisis de incidentes.
- Revisión de denuncias.
- Seguimiento de acciones correctivas.

La finalidad es obtener información que permita determinar si el sistema es adecuado y dónde necesita fortalecerse.

Mejora continua

La **mejora continua** es un principio fundamental de los sistemas de gestión.

Cuando una organización identifica una deficiencia, un incumplimiento o un incidente, debe analizar sus causas y determinar qué medidas son necesarias para evitar que vuelva a ocurrir.

Esto puede implicar:

- Modificar procedimientos.
- Fortalecer controles.
- Actualizar políticas.
- Capacitar nuevamente al personal.
- Revisar proveedores o terceros.
- Modificar responsabilidades.
- Actualizar la evaluación de riesgos.

De esta manera, el sistema evoluciona junto con la organización y con los cambios de su entorno.

Estructura de alto nivel y compatibilidad con otras normas ISO

La estructura de ISO 37001 facilita su integración con otros sistemas de gestión basados en normas ISO.

Esto resulta especialmente útil para organizaciones que ya cuentan con sistemas relacionados con:

- **ISO 9001**, para gestión de la calidad.
- **ISO 14001**, para gestión ambiental.
- **ISO 45001**, para seguridad y salud en el trabajo.
- **ISO 37301**, para sistemas de gestión de compliance.

La integración permite evitar la duplicación innecesaria de procesos y aprovechar estructuras existentes de **gestión de riesgos, auditoría, documentación, capacitación, revisión por la dirección y mejora continua**.

ISO 37001 y ISO 37301

Es importante diferenciar especialmente **ISO 37001** de **ISO 37301**. ISO 37001 está específicamente dedicada al **Sistema de Gestión Antisoborno**.

ISO 37301, en cambio, tiene un alcance más amplio y está orientada a los **Sistemas de Gestión de Compliance**, es decir, a la gestión de diferentes obligaciones de cumplimiento de una organización.

Por esta razón, una organización puede utilizar ambas normas de manera complementaria.

ISO 37001 permite profundizar específicamente en la prevención y gestión del **soborno**, mientras que ISO 37301 puede proporcionar un marco más amplio para gestionar el conjunto de obligaciones de compliance de la organización.

Certificación y sistema de gestión

ISO 37001 es una norma que puede utilizarse como referencia para implementar un sistema de gestión y también puede servir como base para un **proceso de certificación por un organismo de certificación competente**.

Sin embargo, debe diferenciarse claramente entre **capacitación, implementación y certificación**. Una persona que realiza un curso sobre ISO 37001 adquiere conocimientos sobre la norma, pero eso no significa que la organización donde trabaja esté certificada.

De la misma manera, una organización puede implementar elementos de ISO 37001 sin necesariamente haber obtenido una certificación externa.

La certificación implica una **evaluación independiente del sistema de gestión** realizada por un organismo de certificación correspondiente.

¿Qué no garantiza ISO 37001?

La ISO 37001 no garantiza que nunca se produzca un acto de soborno dentro de una organización. Ningún sistema de gestión puede eliminar completamente todos los riesgos.

Su función es establecer un **marco sistemático para gestionar dichos riesgos**, reduciendo la posibilidad de que ocurran y proporcionando mecanismos para detectarlos y responder ante ellos.

Tampoco significa que una organización certificada quede automáticamente exenta de responsabilidad legal. La organización continúa siendo responsable de **cumplir las leyes aplicables** y de mantener funcionando adecuadamente su sistema.

Alcance práctico de la norma

El alcance de ISO 37001 puede abarcar diferentes procesos y actividades de una organización.

Una organización puede determinar el alcance de su sistema considerando:

- Sus actividades.
- Sus unidades organizativas.
- Sus ubicaciones.
- Sus procesos.
- Sus relaciones con terceros.
- Sus riesgos de soborno.
- Sus obligaciones aplicables.

El alcance debe ser suficientemente claro para determinar **qué partes de la organización y qué actividades están comprendidas dentro del Sistema de Gestión Antisoborno**.

Importancia para las organizaciones peruanas

Para las organizaciones que operan en Perú, ISO 37001 puede convertirse en una herramienta de apoyo para fortalecer sus sistemas de integridad y cumplimiento.

Su utilidad es especialmente relevante en sectores donde existen relaciones frecuentes con:

Entidades públicas, funcionarios, proveedores, contratistas, intermediarios, socios de negocio y procesos de contratación estatal.

En sectores como **minería, construcción, energía, infraestructura y servicios**, la evaluación de riesgos puede adquirir especial importancia debido a la naturaleza de determinadas operaciones y a la interacción con diferentes partes interesadas.

Sin embargo, cada organización debe realizar su propia evaluación y evitar asumir que todos los riesgos son iguales.

Principales características de ISO 37001:2025

La versión actualmente vigente presenta un enfoque integral basado en la gestión sistemática del riesgo de soborno.

Entre sus características principales se encuentran:

- **Aplicación a organizaciones públicas, privadas y sin fines de lucro**.
- Gestión de diferentes formas de soborno, incluidos riesgos de **soborno directo e indirecto**.
- Enfoque basado en riesgos.
- Importancia del liderazgo y compromiso de la alta dirección.
- Política antisoborno.
- Función antisoborno.
- Debida diligencia.
- Controles financieros y no financieros.
- Capacitación y comunicación.
- Mecanismos de denuncia.
- Investigación de posibles incidentes.
- Auditoría y evaluación del desempeño.
- Revisión por la dirección.
- Acciones correctivas.
- **Mejora continua**.

ISO 37001:2016 frente a ISO 37001:2025

Para evitar confusiones, es importante recordar que **ISO 37001:2016 ya no es la edición vigente**. La primera edición fue publicada en 2016 y posteriormente retirada.

La **ISO 37001:2025 es la segunda edición y fue publicada el 28 de febrero de 2025**. Actualmente es la referencia internacional vigente para los Sistemas de Gestión Antisoborno.

Por ello, los materiales de capacitación, procedimientos y referencias utilizados por una organización deberían comprobar siempre **qué edición de la norma están utilizando**.

Importancia de la actualización 2025

La actualización de 2025 demuestra que las normas de gestión no son documentos estáticos.

Las organizaciones enfrentan nuevos riesgos, cambian sus modelos de negocio, utilizan nuevas tecnologías y desarrollan relaciones comerciales cada vez más complejas.

La nueva edición incorpora mejoras y aclaraciones relacionadas con la **cultura de cumplimiento, conflictos de interés, función antisoborno y otros aspectos del sistema**, buscando mantener la norma alineada con las prácticas actuales y con otros estándares de gestión.

Por esta razón, una organización que anteriormente trabajaba con ISO 37001:2016 debe considerar los cambios introducidos por la edición 2025 y determinar las acciones necesarias para mantener la conformidad de su sistema.

Aspectos clave para recordar

La **ISO 37001:2025 es una norma internacional dedicada específicamente a los Sistemas de Gestión Antisoborno**.

Su propósito es ayudar a las organizaciones a **prevenir, detectar y responder ante el soborno**, así como a gestionar las obligaciones antisoborno aplicables a sus actividades.

La norma puede aplicarse a organizaciones **públicas, privadas y sin fines de lucro**, independientemente de su sector, siempre que se adapte adecuadamente a su contexto y riesgos.

Su estructura sigue el enfoque de los sistemas modernos de gestión y comprende elementos relacionados con **contexto, liderazgo, planificación, apoyo, operación, evaluación del desempeño y mejora**.

ISO 37001 no sustituye la legislación nacional. En el caso de las organizaciones que operan en Perú, debe complementarse con el **marco jurídico peruano aplicable**.

Finalmente, debe mantenerse una distinción clara entre **conocer la norma, implementar un sistema de gestión y obtener una certificación**. Son tres conceptos diferentes y cada uno implica responsabilidades y procesos distintos.

La comprensión de estos fundamentos permitirá analizar en los siguientes apartados cómo funciona el **ciclo PHVA, cuáles son los términos esenciales de ISO 37001 y cómo se relaciona esta norma con otros sistemas de gestión ISO**.

2.2. Ciclo PHVA aplicado al antisoborno

Introducción al ciclo PHVA

El **ciclo PHVA**, también conocido como **Planificar – Hacer – Verificar – Actuar**, constituye un enfoque fundamental para gestionar y mejorar continuamente los sistemas de gestión. En inglés se conoce como **PDCA: Plan – Do – Check – Act**.

En el contexto de la **ISO 37001:2025**, el ciclo PHVA permite organizar el Sistema de Gestión Antisoborno como un proceso continuo. La organización no debe limitarse a crear una política antisoborno y establecer algunos controles, sino que debe **planificar el sistema, implementarlo, comprobar su funcionamiento y realizar mejoras cuando sea necesario**. ISO confirma que la norma está diseñada para establecer, implementar, mantener y mejorar un Sistema de Gestión Antisoborno destinado a prevenir, detectar y responder ante el soborno.

El ciclo puede representarse mediante cuatro etapas:

- **Planificar (P):** determinar qué se necesita hacer y cómo se gestionarán los riesgos.
- **Hacer (H):** implementar los procesos, controles y medidas planificadas.
- **Verificar (V):** comprobar si el sistema funciona y si alcanza los resultados previstos.
- **Actuar (A):** corregir las deficiencias y mejorar continuamente el sistema.

Estas cuatro etapas **no funcionan de manera aislada**. Al finalizar una vuelta del ciclo, los resultados obtenidos sirven como información para iniciar una nueva etapa de planificación.

El PHVA como sistema continuo

El principal valor del ciclo PHVA es que transforma la gestión antisoborno en un **proceso dinámico y permanente**.

Los riesgos de una organización pueden cambiar. Pueden aparecer nuevos proveedores, nuevos mercados, nuevos proyectos, nuevas relaciones con funcionarios públicos, nuevas modalidades de contratación o cambios en la legislación.

Por ello, un control que era adecuado hace algunos años puede dejar de ser suficiente.

El ciclo PHVA permite que la organización pueda:

- Identificar nuevos riesgos.
- Revisar la eficacia de los controles existentes.
- Detectar deficiencias.
- Incorporar cambios legales o regulatorios.
- Actualizar procedimientos.
- Capacitar nuevamente al personal.
- Mejorar los controles financieros y no financieros.
- Fortalecer la cultura antisoborno.
- **Adaptar el sistema a los cambios de la organización.**

De esta manera, el Sistema de Gestión Antisoborno se convierte en un mecanismo de **mejora continua**, y no en un conjunto de documentos creados únicamente para cumplir una formalidad.

Primera etapa: Planificar

La etapa de **Planificar** consiste en determinar qué necesita hacer la organización para establecer y gestionar adecuadamente su Sistema de Gestión Antisoborno.

En esta etapa se analiza el contexto de la organización, sus actividades, sus partes interesadas, sus obligaciones aplicables y los riesgos relacionados con el soborno.

La planificación permite responder preguntas como:

¿Dónde estamos expuestos al soborno?

¿Qué personas, procesos o relaciones presentan mayor riesgo?

¿Qué controles necesitamos?

¿Quién será responsable?

¿Qué objetivos queremos alcanzar?

¿Cómo comprobaremos posteriormente que el sistema funciona?

Esta etapa proporciona la base sobre la cual se desarrollarán las demás actividades del sistema.

Comprensión del contexto

Una organización no puede gestionar correctamente sus riesgos si primero no comprende su propio contexto. Debe analizar factores internos y externos que puedan afectar su capacidad para alcanzar los objetivos del Sistema de Gestión Antisoborno.

Entre estos factores pueden encontrarse:

- Naturaleza y tamaño de la organización.
- Estructura organizacional.
- Actividades desarrolladas.
- Mercados donde opera.
- Ubicaciones geográficas.
- Tipo de clientes.
- Relaciones con entidades públicas.
- Proveedores y contratistas.
- Intermediarios y agentes.
- Requisitos legales.
- Obligaciones contractuales.
- Riesgos propios del sector económico.

Por ejemplo, una empresa minera que gestiona permisos, contratistas, proveedores y relaciones con autoridades puede tener una exposición al soborno diferente a la de una empresa dedicada exclusivamente al comercio minorista.

Por ello, **la planificación debe comenzar desde la realidad de la organización y no desde un modelo genérico**.

Identificación y evaluación de riesgos

Uno de los elementos más importantes de la planificación es la **evaluación de los riesgos de soborno**.

La organización debe identificar dónde podría producirse un soborno, quién podría estar involucrado, qué tipo de ventaja indebida podría utilizarse y qué consecuencias podría generar el incidente.

Algunos procesos que pueden requerir especial atención son:

- Contrataciones y adquisiciones.
- Selección de proveedores.
- Contratación de intermediarios.
- Relaciones con funcionarios públicos.
- Obtención de permisos y licencias.
- Fiscalización e inspecciones.
- Contratos comerciales.
- Donaciones y patrocinios.
- Regalos y hospitalidad.
- Pagos y operaciones financieras.

La evaluación debe permitir establecer **prioridades**. No todos los riesgos tienen necesariamente el mismo nivel de probabilidad o impacto, por lo que los recursos deben concentrarse de manera proporcional.

Definición de objetivos antisoborno

La planificación también implica establecer **objetivos antisoborno**. Los objetivos deben ser coherentes con la política antisoborno y con los riesgos identificados.

Por ejemplo, una organización podría establecer objetivos relacionados con:

- Capacitación del personal expuesto a riesgos.
- Evaluación de terceros de alto riesgo.
- Fortalecimiento de controles financieros.
- Reducción de incumplimientos detectados.
- Implementación de nuevos controles.
- Tiempo de respuesta ante denuncias.
- Realización de auditorías internas.
- Actualización periódica de la evaluación de riesgos.

Los objetivos deben ser suficientemente claros para que posteriormente sea posible **verificar si fueron alcanzados**.

Segunda etapa: Hacer

La etapa **Hacer** consiste en poner en práctica lo que fue planificado. Aquí la organización implementa sus políticas, procedimientos, controles y mecanismos de prevención.

Esta etapa transforma la planificación en **acciones concretas dentro de las operaciones diarias**.

Entre las actividades pueden encontrarse:

- Comunicación de la política antisoborno.
- Capacitación del personal.
- Debida diligencia de socios de negocio.
- Aplicación de controles financieros.
- Aplicación de controles no financieros.
- Gestión de regalos y hospitalidad.
- Procedimientos de aprobación.
- Canales de denuncia.
- Investigación de posibles incidentes.
- Supervisión de terceros.
- Conservación de información documentada.

ISO identifica precisamente como componentes relevantes del sistema las **políticas antisoborno, la debida diligencia, los controles financieros y no financieros, la capacitación y los mecanismos de seguimiento, reporte y mejora**.

Implementación de la política antisoborno

La política antisoborno debe pasar de ser un documento formal a convertirse en una **regla aplicable a las actividades de la organización**. Los trabajadores deben conocerla y comprender cómo se relaciona con sus funciones.

Por ejemplo, una política puede establecer prohibiciones respecto de determinados pagos, regalos o beneficios, pero también debe indicar qué debe hacer un trabajador cuando recibe una solicitud indebida o cuando sospecha que un tercero está intentando influir en una decisión.

La eficacia de la política depende, por tanto, de su **integración en los procesos reales de la organización**.

Capacitación y sensibilización

La capacitación forma parte de la implementación práctica del sistema. No todas las personas necesitan necesariamente el mismo nivel de formación. La organización debe considerar las funciones y los riesgos de cada grupo.

Por ejemplo:

Un trabajador administrativo puede necesitar conocer las reglas generales sobre regalos, conflictos de interés y denuncias.

Un comprador puede requerir mayor formación sobre **selección de proveedores, conflictos de interés y controles de contratación**.

Un gerente que mantiene relaciones con funcionarios públicos puede necesitar una formación más profunda sobre **interacciones con autoridades, hospitalidad, terceros y riesgos de soborno**.

La capacitación debe permitir que las personas **reconozcan situaciones de riesgo y sepan cómo actuar**.

Debida diligencia

Durante la etapa de implementación, la organización aplica procedimientos de **debida diligencia** sobre determinadas personas y organizaciones.

La intensidad de la debida diligencia debe guardar relación con el nivel de riesgo.

Puede incluir, dependiendo del caso:

- Identificación del tercero.
- Verificación de información corporativa.
- Revisión de antecedentes.
- Evaluación de reputación.
- Identificación de posibles conflictos de interés.
- Revisión de propietarios o beneficiarios cuando sea relevante.
- Evaluación de la naturaleza de los servicios.
- Revisión de honorarios y condiciones comerciales.
- Inclusión de cláusulas antisoborno.

El objetivo no es crear una investigación innecesariamente compleja sobre cada proveedor, sino **aplicar controles adecuados al riesgo identificado**.

Controles financieros y no financieros

La etapa Hacer también implica poner en funcionamiento controles destinados a reducir la posibilidad de soborno.

Los **controles financieros** pueden incluir:

- Aprobación de pagos.
- Separación de funciones.
- Revisión de facturas.
- Conciliaciones.
- Límites de autorización.
- Control de gastos.

- Revisión de operaciones inusuales.

Los **controles no financieros** pueden incluir:

- Procedimientos de contratación.
- Evaluación de proveedores.
- Autorización de regalos y hospitalidad.
- Debida diligencia.
- Gestión de conflictos de interés.
- Controles sobre intermediarios.
- Procedimientos de selección de personal.

La combinación de ambos tipos de controles permite abordar el riesgo desde diferentes perspectivas.

Tercera etapa: Verificar

La etapa **Verificar** consiste en comprobar si el sistema está funcionando de acuerdo con lo planificado. No basta con afirmar que existe una política o que se realizó una capacitación.

La organización debe obtener **evidencia objetiva** de que los procesos y controles se están aplicando y de que son eficaces para gestionar los riesgos identificados.

Entre las actividades de verificación pueden encontrarse:

- Seguimiento de indicadores.
- Evaluación de controles.
- Auditorías internas.
- Revisión de denuncias.
- Análisis de incidentes.
- Revisión del cumplimiento de procedimientos.
- Evaluación de terceros.
- Revisión por la dirección.

Seguimiento de indicadores

Los indicadores pueden ayudar a determinar si el sistema está alcanzando los resultados esperados.

Por ejemplo, una organización puede realizar seguimiento de:

- Porcentaje de trabajadores capacitados.
- Número de terceros evaluados.
- Porcentaje de terceros de alto riesgo sometidos a debida diligencia.
- Número de denuncias recibidas.
- Tiempo promedio de atención de denuncias.
- Número de controles revisados.
- Número de incumplimientos detectados.
- Acciones correctivas pendientes.
- Resultados de auditorías.

Los indicadores deben utilizarse para **tomar decisiones**, no simplemente para producir estadísticas.

Auditoría interna

La **auditoría interna** constituye una herramienta importante de verificación. Su finalidad es evaluar si el sistema cumple los requisitos aplicables y si está implementado y funcionando de manera eficaz.

Una auditoría puede revisar, por ejemplo:

- La política antisoborno.
- La evaluación de riesgos.
- La capacitación.
- Los controles financieros.
- La debida diligencia.
- Los procedimientos de denuncia.
- Los registros.
- La gestión de incidentes.
- Las acciones correctivas.

El resultado puede revelar **conformidades, incumplimientos, debilidades y oportunidades de mejora**.

Revisión por la dirección

La alta dirección debe recibir información suficiente para conocer el desempeño del Sistema de Gestión Antisoborno.

La revisión puede considerar:

- Resultados de auditorías.
- Estado de los objetivos.
- Cambios en los riesgos.
- Incidentes y denuncias.
- Resultados de controles.
- Acciones correctivas.
- Cambios en el contexto.
- Necesidades de recursos.
- Oportunidades de mejora.

Esto permite que la dirección tome decisiones sobre el futuro del sistema y demuestre que la gestión antisoborno forma parte de la **gobernanza de la organización**.

Cuarta etapa: Actuar

La última etapa del ciclo es **Actuar**.

Cuando la organización detecta una deficiencia, debe determinar qué medidas son necesarias para corregirla y evitar, cuando sea posible, que vuelva a producirse.

Esta etapa puede incluir:

- Corrección de incumplimientos.
- Análisis de causas.
- Acciones correctivas.
- Actualización de procedimientos.
- Fortalecimiento de controles.
- Capacitación adicional.
- Revisión de terceros.
- Actualización de la evaluación de riesgos.
- Modificación de objetivos.
- Asignación de nuevos recursos.

El objetivo no es simplemente **"solucionar el problema"**, sino aprender del problema y mejorar el sistema.

Diferencia entre corrección y acción correctiva

Es importante diferenciar ambos conceptos. Una **corrección** busca solucionar una situación detectada.

Una **acción correctiva** busca eliminar la causa de una no conformidad para evitar que vuelva a ocurrir o para reducir la posibilidad de recurrencia.

Por ejemplo, si se detecta que un trabajador realizó una capacitación obligatoria fuera del plazo, la corrección podría consistir en completar inmediatamente la capacitación.

Pero si se descubre que varias personas incumplieron el plazo porque el sistema de seguimiento no genera alertas, una acción correctiva podría consistir en **modificar el proceso de seguimiento y establecer un mecanismo automático de control**.

El ciclo vuelve a comenzar

Una vez aplicadas las acciones de mejora, la organización vuelve a la etapa de **Planificar**.

La nueva información obtenida puede modificar:

- El contexto.
- La evaluación de riesgos.
- Los objetivos.
- Los controles.
- Los procedimientos.
- Los recursos.
- Las necesidades de capacitación.

Por ello, el PHVA debe entenderse como un **ciclo continuo**.

No existe un punto en el que la organización pueda afirmar definitivamente que su sistema está terminado. El sistema debe evolucionar conforme cambian los riesgos y las circunstancias.

Ejemplo práctico: riesgo de soborno en una contratación

Para comprender mejor el ciclo PHVA, puede utilizarse el ejemplo de una empresa que participa en una contratación con una entidad pública.

En la etapa **Planificar**, la organización identifica que el proceso presenta riesgo de soborno debido al contacto con funcionarios, el valor del contrato y la participación de intermediarios. Se evalúa el riesgo y se establecen controles específicos.

En la etapa **Hacer**, la empresa implementa dichos controles. Realiza la debida diligencia del intermediario, establece reglas para las interacciones con funcionarios, exige autorizaciones para determinados gastos y capacita al personal involucrado.

En la etapa **Verificar**, la organización revisa si los controles fueron aplicados. Se analiza la documentación, se revisan los pagos y se realiza una auditoría interna.

Durante la revisión se descubre que determinados gastos relacionados con el intermediario fueron aprobados sin la documentación requerida.

En la etapa **Actuar**, la organización analiza la causa, corrige la situación, fortalece el procedimiento de aprobación y capacita nuevamente a las personas involucradas.

Posteriormente, el nuevo procedimiento vuelve a ser evaluado. De esta manera, **el incidente se convierte en una fuente de aprendizaje y mejora para el sistema**.

Ejemplo práctico: regalos y hospitalidad

Supongamos que una organización identifica durante su evaluación de riesgos que determinados trabajadores mantienen contacto frecuente con funcionarios públicos.

En la etapa **Planificar**, se establece un procedimiento para controlar regalos y hospitalidad.

En la etapa **Hacer**, se implementa un sistema de autorización y registro de determinados beneficios.

En la etapa **Verificar**, se revisan los registros y se detecta que algunas invitaciones no fueron reportadas correctamente.

En la etapa **Actuar**, se analiza por qué los trabajadores no realizaron los reportes y se determina que el procedimiento era poco claro.

La organización actualiza el procedimiento, mejora la capacitación y establece un mecanismo de seguimiento. El ciclo comienza nuevamente con la revisión de la eficacia de estas medidas.

PHVA y cultura antisoborno

El ciclo PHVA no debe entenderse únicamente como una herramienta técnica. También contribuye al desarrollo de una **cultura organizacional de integridad**.

Una organización que evalúa constantemente sus riesgos, escucha las preocupaciones de sus trabajadores, investiga incidentes y aprende de sus errores demuestra que la prevención del soborno forma parte de su gestión habitual.

La cultura antisoborno se fortalece cuando las personas observan que:

Las reglas se aplican de manera coherente.

Las denuncias son tomadas en serio.

Los controles funcionan.

La dirección participa activamente.

Los incumplimientos generan acciones correctivas.

Los procedimientos se mejoran cuando dejan de ser eficaces.

PHVA y gestión basada en riesgos

El ciclo PHVA está estrechamente relacionado con el **enfoque basado en riesgos**.

La organización identifica y evalúa sus riesgos durante la planificación, implementa controles para tratarlos, verifica su eficacia y utiliza los resultados para determinar si es necesario modificar las medidas adoptadas.

Esto genera una relación continua:

Riesgo → Control → Verificación → Mejora → Nueva evaluación del riesgo.

Por ejemplo, si una empresa comienza a trabajar con un nuevo intermediario en un país donde la exposición al soborno es considerada elevada, el contexto puede cambiar y será necesario revisar la evaluación de riesgos y determinar si los controles existentes siguen siendo adecuados.

PHVA en organizaciones públicas y privadas

El ciclo puede aplicarse tanto a **organizaciones públicas como privadas**. En una entidad pública puede utilizarse para gestionar riesgos relacionados con contrataciones, permisos, licencias, fiscalización, autorizaciones y relaciones con proveedores.

En una empresa privada puede aplicarse a compras, ventas, contratación de intermediarios, relaciones con clientes, contratistas, proveedores y funcionarios públicos.

Lo importante es adaptar el ciclo a **las características, procesos y riesgos reales de cada organización**.

Relación del PHVA con ISO 37001:2025

La estructura de ISO 37001:2025 puede analizarse utilizando el enfoque PHVA.

De manera general:

Planificar se relaciona principalmente con el contexto, la planificación y la identificación y tratamiento de riesgos.

Hacer comprende la implementación de los recursos, competencias, comunicación y controles operativos.

Verificar comprende la evaluación del desempeño, seguimiento, medición, auditoría y revisión por la dirección.

Actuar comprende el tratamiento de las no conformidades, las acciones correctivas y la mejora continua.

El liderazgo atraviesa las diferentes etapas porque la **alta dirección debe mantener su compromiso y supervisión durante todo el funcionamiento del sistema**. Esta correspondencia puede observarse en la estructura de requisitos de ISO 37001:2025.

Errores frecuentes en la aplicación del PHVA

Una organización puede implementar formalmente un sistema y, sin embargo, no aplicar correctamente el ciclo PHVA.

Entre los errores más frecuentes se encuentran:

- Elaborar una política antisoborno y no actualizarla.
- Realizar una evaluación de riesgos una sola vez.
- Implementar controles sin comprobar su eficacia.
- Capacitar al personal sin evaluar si la capacitación produjo resultados.
- Realizar auditorías sin aplicar acciones correctivas.
- Recibir denuncias sin analizar las causas de los problemas.
- Mantener procedimientos que ya no corresponden a las actividades actuales.
- No involucrar a la alta dirección.
- Considerar la certificación como el objetivo final del sistema.

Estos errores pueden convertir el sistema en un **modelo documental**, en lugar de un sistema de gestión realmente operativo.

Aplicación del PHVA en una organización peruana

Para una organización que opera en Perú, el ciclo PHVA también puede utilizarse para mantener actualizado el sistema frente a cambios en el **marco legal y regulatorio nacional**.

Por ejemplo, cuando cambia una norma relacionada con responsabilidad de las personas jurídicas o prevención de delitos, la organización puede:

Planificar: analizar el cambio y determinar qué procesos pueden verse afectados.

Hacer: actualizar políticas, procedimientos y controles.

Verificar: comprobar que los trabajadores conocen los nuevos requisitos y que los controles se aplican correctamente.

Actuar: corregir las deficiencias identificadas y realizar nuevas mejoras.

Esto permite integrar la evolución normativa dentro del propio sistema de gestión.

Beneficios del ciclo PHVA

La aplicación adecuada del ciclo PHVA puede ayudar a una organización a:

- **Reducir y gestionar los riesgos de soborno**.
- Detectar debilidades antes de que generen consecuencias mayores.
- Mejorar los controles internos.
- Fortalecer la responsabilidad de la dirección.
- Mantener actualizados los procedimientos.
- Mejorar la capacitación.
- Utilizar los resultados de auditorías para generar mejoras.
- Adaptarse a cambios en el entorno.
- Fortalecer la cultura de integridad.
- Integrar la gestión antisoborno con otros sistemas de gestión.

ISO señala que la gestión antisoborno debe entenderse como un sistema que puede establecerse, implementarse, mantenerse y **mejorarse continuamente**, y que puede funcionar de manera independiente o integrarse con otros sistemas de gestión.

Aspectos clave para recordar

El **ciclo PHVA es una herramienta fundamental para comprender cómo funciona un Sistema de Gestión Antisoborno**.

Su lógica puede resumirse de la siguiente manera:

Planificar: comprender el contexto, identificar los riesgos, establecer objetivos y determinar controles.

Hacer: implementar políticas, procedimientos, capacitación, debida diligencia y controles.

Verificar: medir resultados, realizar seguimiento, auditorías y revisiones de la dirección.

Actuar: corregir problemas, aplicar acciones correctivas y mejorar el sistema.

El ciclo no termina después de la primera implementación. **La última etapa alimenta nuevamente la planificación**, generando un proceso continuo de aprendizaje y mejora.

En una organización eficaz, el PHVA permite que la gestión antisoborno deje de ser una actividad aislada y se convierta en **parte integral de la gestión, las operaciones y la toma de decisiones**. Esta lógica es coherente con el enfoque de ISO 37001:2025, cuyo propósito es ayudar a las organizaciones a prevenir, detectar y responder ante el soborno mediante un sistema de gestión estructurado y sujeto a mejora continua.

2.3. Términos y definiciones clave

Introducción

El conocimiento de los **términos y definiciones de ISO 37001** es fundamental para comprender correctamente los requisitos de un Sistema de Gestión Antisoborno. La norma utiliza conceptos específicos que permiten establecer un lenguaje común dentro de la organización y evitar interpretaciones diferentes entre la alta dirección, la función antisoborno, los trabajadores, auditores y socios de negocio.

La versión actualmente vigente es **ISO 37001:2025**, segunda edición, publicada en febrero de 2025. Esta versión establece requisitos y orientación para establecer, implementar, mantener y mejorar un Sistema de Gestión Antisoborno aplicable a organizaciones públicas, privadas y sin fines de lucro.

Comprender las definiciones es especialmente importante porque conceptos como **soborno, riesgo de soborno, debida diligencia, socio de negocio, personal, función antisoborno y sistema de gestión antisoborno** aparecen directamente relacionados con la implementación práctica de la norma.

Soborno

El concepto central de ISO 37001 es el **soborno**.

En términos generales, la norma utiliza el concepto para referirse a la **oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida**, de cualquier valor, ya sea de manera directa o indirecta, cuando se realiza en relación con el desempeño de las funciones de una persona y en contravención de la legislación aplicable.

La ventaja indebida no tiene que ser necesariamente dinero.

Puede tratarse de una ventaja:

- **Financiera**, como dinero, pagos, comisiones o beneficios económicos.
- **No financiera**, como determinados regalos, favores, beneficios personales u otras ventajas.
- Directa o indirecta.
- Ofrecida o recibida a través de un tercero.

Por ello, el análisis de un posible soborno debe considerar **la finalidad, las circunstancias, la naturaleza de la ventaja y las obligaciones legales aplicables**, y no solamente el valor monetario del beneficio.

Soborno directo e indirecto

ISO 37001 contempla tanto el **soborno directo como el soborno indirecto**.

El soborno directo ocurre cuando la persona u organización entrega, ofrece o solicita directamente una ventaja indebida.

El soborno indirecto puede producirse cuando interviene un **tercero o intermediario**.

Por ejemplo, una organización podría intentar utilizar a un consultor para entregar una ventaja indebida a una persona que toma decisiones comerciales o administrativas. El hecho de que el pago sea realizado por el consultor y no directamente por la organización **no elimina necesariamente el riesgo de soborno**.

Esta es una de las razones por las cuales ISO 37001 presta especial atención a los **socios de negocio y a la debida diligencia**.

Soborno activo y soborno pasivo

Otro concepto importante es la diferencia entre **soborno activo y soborno pasivo**.

El soborno activo se relaciona con quien **ofrece, promete o entrega** una ventaja indebida.

El soborno pasivo se relaciona con quien **solicita o acepta** una ventaja indebida.

ISO 37001 contempla ambos escenarios y reconoce que el riesgo puede producirse tanto cuando una organización intenta influir indebidamente en otra persona como cuando alguien intenta obtener una ventaja indebida aprovechándose de su posición.

Por esta razón, un sistema antisoborno debe proteger a la organización frente a diferentes direcciones del riesgo:

La organización o sus representantes pueden intentar sobornar a otra persona. Una persona puede intentar sobornar a la organización o a sus trabajadores.

Ventaja indebida

La expresión **ventaja indebida** es importante para comprender el concepto de soborno.

Se refiere a un beneficio que no corresponde legítimamente a la persona que lo recibe y que puede utilizarse como incentivo o recompensa para que alguien actúe o deje de actuar en relación con sus funciones.

La ventaja puede ser económica o no económica. Por ello, una organización no debe limitar sus controles exclusivamente al dinero en efectivo.

Dependiendo del contexto, también pueden requerir atención:

- Regalos.
- Viajes.
- Hospitalidad.
- Favores personales.
- Beneficios para familiares.
- Oportunidades laborales.
- Donaciones.
- Patrocinios.
- Otros beneficios.

No todo regalo o beneficio constituye automáticamente un soborno. La organización debe evaluar las circunstancias, la finalidad, el momento, el valor, la frecuencia y las normas aplicables.

Organización

Dentro de ISO 37001, el término **organización** tiene un alcance amplio.

Puede comprender diferentes tipos de entidades que cuentan con funciones, responsabilidades, autoridades y relaciones destinadas a alcanzar determinados objetivos.

Puede tratarse de:

- Una empresa.
- Una sociedad.
- Una corporación.
- Una entidad pública.
- Una institución.
- Una organización sin fines de lucro.
- Una asociación.
- Una parte determinada de una organización más grande.

La definición de organización también permite comprender que ISO 37001 puede aplicarse a **organizaciones de diferentes tamaños, sectores y estructuras**.

Sistema de Gestión Antisoborno

El **Sistema de Gestión Antisoborno (SGAS)** es el conjunto estructurado de elementos mediante los cuales una organización gestiona sus riesgos relacionados con el soborno.

No debe confundirse con una simple política antisoborno. El sistema comprende diferentes componentes que funcionan conjuntamente, como:

- Política antisoborno.
- Liderazgo y responsabilidades.
- Evaluación de riesgos.
- Objetivos.
- Controles.
- Debida diligencia.
- Capacitación.
- Comunicación.
- Denuncias.
- Investigación.
- Seguimiento.
- Auditoría.
- Revisión por la dirección.
- Acciones correctivas.
- **Mejora continua**.

ISO establece que el sistema está diseñado para ayudar a las organizaciones a **prevenir, detectar y responder ante el soborno**.

Riesgo de soborno

El **riesgo de soborno** representa la posibilidad de que se produzca una situación de soborno que pueda afectar a la organización.

La identificación de estos riesgos constituye una actividad esencial del sistema. La organización debe considerar sus actividades, relaciones y circunstancias particulares para determinar dónde existe mayor exposición.

Por ejemplo, pueden existir riesgos asociados con:

- Contrataciones públicas.
- Proveedores.
- Contratistas.
- Agentes.
- Intermediarios.
- Regalos y hospitalidad.
- Donaciones.
- Pagos.
- Licencias.
- Permisos.
- Inspecciones.
- Relaciones comerciales.

El nivel de riesgo puede variar significativamente entre organizaciones e incluso entre diferentes áreas de una misma organización.

Evaluación del riesgo de soborno

La **evaluación del riesgo de soborno** es el proceso mediante el cual la organización identifica y analiza los riesgos relacionados con sus actividades.

El objetivo es determinar **qué riesgos existen, qué tan relevantes son y qué controles deben establecerse**. Una evaluación adecuada debe considerar las características particulares de la organización y no limitarse a copiar una matriz genérica.

Por ejemplo, una empresa que participa frecuentemente en procesos de contratación pública puede requerir una evaluación detallada de los riesgos asociados con:

- Funcionarios públicos.
- Intermediarios.
- Contratistas.
- Procesos de licitación.
- Regalos y hospitalidad.
- Pagos y comisiones.

Personal

El término **personal** comprende a las personas que trabajan para la organización o que actúan en su nombre, según corresponda al sistema y al contexto de la organización.

Esto puede incluir diferentes niveles y funciones.

Por ejemplo:

- Alta dirección.
- Gerentes.
- Trabajadores administrativos.
- Personal operativo.
- Personal temporal.
- Personas que desempeñan funciones relacionadas con las actividades de la organización.

El riesgo de soborno no depende únicamente del cargo de una persona. Debe considerarse **la función que desempeña y el nivel de exposición al riesgo**.

Por ello, una organización puede establecer diferentes niveles de capacitación y controles dependiendo de las responsabilidades de cada grupo.

Alta dirección

La **alta dirección** tiene un papel fundamental dentro del Sistema de Gestión Antisoborno. La prevención del soborno no puede quedar exclusivamente en manos del área legal o de cumplimiento.

La dirección debe demostrar **liderazgo y compromiso** con el sistema, promover una cultura de integridad y proporcionar los recursos necesarios para que el sistema pueda

funcionar adecuadamente. La conducta de la dirección tiene además un efecto importante sobre la cultura organizacional.

Si los trabajadores observan que la dirección respeta las políticas y rechaza las prácticas indebidas incluso cuando pueden representar una ventaja comercial, el mensaje de integridad adquiere mayor credibilidad.

Función antisoborno

La **función antisoborno** es la función o persona encargada de determinadas responsabilidades relacionadas con la gestión del sistema antisoborno. Su finalidad es contribuir a que el sistema se implemente y mantenga adecuadamente y que la organización cuente con una supervisión apropiada de sus medidas antisoborno.

Dependiendo del tamaño y estructura de la organización, esta función puede organizarse de diferentes maneras. En una organización pequeña puede existir una persona con responsabilidades específicas.

En una organización grande puede existir una **estructura especializada de cumplimiento antisoborno**. Lo importante es que las responsabilidades estén claramente definidas y que la función cuente con la autoridad, competencia y acceso necesarios para desempeñar sus responsabilidades.

Socio de negocio

Uno de los conceptos especialmente importantes en ISO 37001:2025 es **socio de negocio**.

El término hace referencia a una parte externa con la que la organización mantiene o pretende establecer algún tipo de relación comercial o empresarial.

La definición es deliberadamente amplia y puede incluir:

- Clientes.
- Proveedores.
- Contratistas.
- Consultores.
- Subcontratistas.
- Agentes.
- Distribuidores.
- Representantes.
- Intermediarios.
- Socios de empresas conjuntas.
- Socios de consorcios.
- Proveedores de servicios externalizados.
- Inversionistas.

No todos los socios de negocio presentan necesariamente el mismo nivel de riesgo. La organización debe considerar **el tipo de relación y la posibilidad de exposición al soborno**.

Debida diligencia

La **debida diligencia** es el proceso mediante el cual la organización obtiene y analiza información relevante antes de establecer determinadas relaciones o realizar determinadas operaciones, y cuando corresponda durante la relación.

Su finalidad es ayudar a identificar y gestionar riesgos. En materia antisoborno, la debida diligencia puede incluir la revisión de:

- Identidad del tercero.
- Estructura de propiedad.
- Reputación.
- Antecedentes relevantes.
- Relaciones con funcionarios públicos.
- Conflictos de interés.
- Naturaleza de los servicios.
- Condiciones económicas.
- Nivel de riesgo asociado a la relación.

La profundidad de la investigación debe ser **razonable y proporcional al riesgo**.

No tendría sentido aplicar exactamente el mismo procedimiento a todos los proveedores independientemente de su tamaño, función y exposición al riesgo.

Controles financieros

Los **controles financieros** son mecanismos destinados a reducir el riesgo de que las operaciones financieras sean utilizadas para facilitar u ocultar un soborno.

Pueden incluir:

- Autorización de pagos.
- Separación de funciones.
- Límites de aprobación.
- Revisión de facturas.
- Control de gastos.
- Conciliaciones.
- Registros contables.
- Supervisión de operaciones inusuales.
- Controles sobre comisiones y honorarios.

Su finalidad no es únicamente detectar irregularidades después de que ocurran, sino **reducir las oportunidades de que un pago indebido pueda realizarse o esconderse**.

Controles no financieros

Los **controles no financieros** son aquellos que gestionan riesgos antisoborno fuera de los procesos financieros.

Pueden incluir controles relacionados con:

- Compras.
- Contratación de proveedores.
- Selección de terceros.
- Licitaciones.
- Contratación de personal.
- Regalos y hospitalidad.
- Donaciones.
- Patrocinios.
- Gestión de conflictos de interés.
- Interacciones con funcionarios públicos.

ISO 37001 considera tanto los controles financieros como los **controles no financieros** como componentes relevantes del sistema.

Regalos y hospitalidad

Los **regalos y la hospitalidad** pueden representar áreas de riesgo antisoborno cuando se utilizan para influir indebidamente en una decisión.

Una política de regalos y hospitalidad puede establecer:

- Qué tipos de beneficios están permitidos.
- Qué beneficios están prohibidos.
- Límites de valor.
- Procedimientos de autorización.
- Reglas especiales para funcionarios públicos.
- Requisitos de registro.
- Situaciones que deben ser reportadas.

Es importante comprender que **el valor económico por sí solo no determina necesariamente si existe soborno**. También deben analizarse el contexto, la intención, el momento y la relación entre las partes.

Conflicto de interés

Un **conflicto de interés** puede producirse cuando los intereses personales de una persona pueden interferir, o parecer interferir, con el cumplimiento objetivo de sus responsabilidades. Por ejemplo, una persona encargada de seleccionar proveedores podría tener una relación personal o económica con uno de los proveedores participantes.

El conflicto de interés **no equivale automáticamente a soborno**, pero puede generar un riesgo significativo de decisiones indebidas y debe ser gestionado adecuadamente. Por ello, la identificación y gestión de conflictos de interés forma parte de una cultura de integridad y constituye un aspecto relevante en la evolución de ISO 37001:2025.

Denuncia

La **denuncia** es la comunicación de una preocupación, sospecha o información relacionada con una posible conducta indebida. En un sistema antisoborno, los mecanismos

de denuncia permiten que trabajadores y otras personas puedan comunicar situaciones sospechosas.

Un canal de denuncia eficaz debe proporcionar condiciones adecuadas para que las personas puedan comunicar sus preocupaciones y debe existir un proceso para **recibir, evaluar y gestionar la información**.

La existencia de un canal no es suficiente por sí sola. La organización debe establecer procedimientos para determinar cómo se gestionarán las comunicaciones recibidas.

Investigación

La **investigación** consiste en el proceso mediante el cual la organización analiza una sospecha o un posible incidente para determinar los hechos relevantes.

Una investigación antisoborno debe realizarse de manera adecuada, objetiva y proporcional a la naturaleza del caso.

Puede incluir:

- Recopilación de información.
- Revisión de documentos.
- Análisis de transacciones.
- Entrevistas.
- Revisión de comunicaciones.
- Identificación de personas involucradas.
- Evaluación de controles.

La investigación debe respetar las **leyes y procedimientos aplicables**, así como las garantías y derechos correspondientes.

Incidente de soborno

Un **incidente de soborno** puede referirse a una situación en la que existe evidencia, sospecha o identificación de una conducta relacionada con el soborno. No todos los reportes recibidos necesariamente constituyen un soborno confirmado.

Por ello, la organización debe contar con mecanismos para:

Recibir la información → evaluar la situación → investigar cuando corresponda → determinar las medidas necesarias.

La respuesta debe ser proporcional a la naturaleza y gravedad del caso.

No conformidad

Una **no conformidad** se produce cuando existe un incumplimiento de un requisito aplicable.

Dentro del sistema antisoborno, una no conformidad puede estar relacionada con:

- Un requisito de ISO 37001.
- Un procedimiento interno.
- Una política antisoborno.
- Una obligación legal aplicable.
- Un control establecido.

Por ejemplo, si el procedimiento interno exige realizar una determinada revisión antes de contratar a un tercero de alto riesgo y dicha revisión no se realiza, puede existir una **no conformidad** que deba ser evaluada y tratada.

Acción correctiva

Una **acción correctiva** busca eliminar la causa de una no conformidad para evitar su repetición o reducir la posibilidad de que vuelva a producirse. No debe confundirse con una simple corrección.

Por ejemplo, si se detecta que una factura no fue revisada correctamente, la corrección puede consistir en revisar la factura.

Pero si se descubre que varias facturas presentan el mismo problema porque el procedimiento de aprobación tiene una deficiencia, la acción correctiva puede implicar **modificar el procedimiento, establecer una nueva autorización y capacitar al personal**.

Información documentada

La gestión antisoborno requiere conservar determinada **información documentada** como evidencia de que el sistema funciona.

Puede incluir:

- Políticas.
- Procedimientos.
- Evaluaciones de riesgos.
- Registros de capacitación.
- Evaluaciones de terceros.
- Autorizaciones.
- Registros de denuncias.
- Informes de investigación.
- Resultados de auditorías.
- Acciones correctivas.

La información documentada permite demostrar qué se hizo, quién lo realizó y qué decisiones fueron tomadas.

Parte interesada

Una **parte interesada** es una persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad de la organización.

En el contexto antisoborno pueden existir diferentes partes interesadas, como:

- Trabajadores.
- Clientes.
- Proveedores.
- Entidades públicas.
- Accionistas.
- Socios comerciales.
- Organismos reguladores.
- Comunidades.
- Organizaciones de la sociedad civil.

La identificación de las partes interesadas ayuda a la organización a comprender mejor su contexto y las expectativas relevantes para su sistema.

Cultura antisoborno

La **cultura antisoborno** representa el entorno de valores, comportamientos y prácticas mediante el cual la organización demuestra que el soborno no es aceptable.

Una cultura sólida no depende únicamente de documentos.

Se refleja en decisiones concretas:

- La dirección rechaza prácticas indebidas.
- Los trabajadores pueden comunicar preocupaciones.
- Los controles se aplican independientemente del cargo de la persona.
- Los terceros son evaluados de acuerdo con el riesgo.
- Los incidentes son investigados.
- Las deficiencias generan mejoras.

La ISO destaca que el sistema antisoborno no debe limitarse al cumplimiento formal, sino que también contribuye a fomentar una **cultura de integridad, transparencia y confianza**.

Corrupción y soborno: no son exactamente lo mismo

Es importante diferenciar **corrupción** de **soborno**. El soborno es una forma específica de conducta corrupta.

La corrupción es un concepto más amplio que puede incluir otras conductas, como determinadas formas de malversación, abuso de funciones, tráfico de influencias, enriquecimiento ilícito u otras conductas ilícitas, dependiendo del marco jurídico aplicable.

Por ello, **ISO 37001 se centra específicamente en el soborno**, aunque una organización puede decidir ampliar su sistema de gestión para abordar otros riesgos de corrupción.

Soborno y fraude

El **soborno y el fraude tampoco son conceptos equivalentes**.

El fraude generalmente implica engaño u ocultación con la finalidad de obtener un beneficio indebido o causar una pérdida, mientras que el soborno implica una ventaja indebida relacionada con la actuación o abstención de actuar de una persona en el desempeño de sus funciones.

Una misma situación puede involucrar diferentes riesgos al mismo tiempo. Por ejemplo, una operación podría incluir falsificación de documentos, fraude contable y un pago indebido.

ISO 37001 se concentra en el **riesgo de soborno**. ISO también señala que la norma no aborda específicamente otros ámbitos como fraude, competencia, lavado de activos o determinados delitos relacionados con prácticas corruptas.

Principio de proporcionalidad

La **proporcionalidad** es un concepto fundamental para la implementación del sistema. Los controles deben ser adecuados a la naturaleza y nivel de riesgo de la organización.

Una empresa pequeña con pocos proveedores y operaciones sencillas no necesariamente necesita la misma estructura de controles que una multinacional con miles de proveedores, operaciones internacionales y relaciones frecuentes con funcionarios públicos.

Por ello, el sistema debe buscar un equilibrio entre:

Riesgo identificado → nivel de control → recursos utilizados.

La finalidad es establecer medidas suficientemente eficaces sin crear procesos innecesariamente complejos.

Mejora continua

La **mejora continua** significa que el Sistema de Gestión Antisoborno debe evolucionar a partir de los resultados obtenidos.

Los cambios en el contexto, las nuevas actividades, los incidentes, las auditorías, las denuncias y las modificaciones legales pueden generar la necesidad de actualizar el sistema.

La organización debe utilizar esta información para:

- Revisar riesgos.
- Mejorar controles.
- Actualizar procedimientos.
- Fortalecer la capacitación.
- Modificar objetivos.
- Corregir deficiencias.
- Mejorar la eficacia del sistema.

La mejora continua es uno de los elementos que permite que el SGAS permanezca **activo y adaptado a la realidad de la organización**.

Relación entre los principales conceptos

Los términos estudiados no deben memorizarse como conceptos independientes. En la práctica, forman una **cadena lógica dentro del Sistema de Gestión Antisoborno**.

La organización identifica sus actividades y contexto. Después identifica los **riesgos de soborno**. Para determinados riesgos evalúa a sus **socios de negocio** mediante **debida diligencia**. Posteriormente establece **controles financieros y no financieros**. El **personal** recibe capacitación y conoce la política antisoborno. La **función antisoborno** supervisa determinados aspectos del sistema. Los canales de **denuncia** permiten comunicar posibles situaciones indebidas. Cuando corresponde, se realiza una **investigación**. Los resultados pueden generar **no conformidades y acciones correctivas**.

Finalmente, la organización utiliza la información obtenida para aplicar la **mejora continua**.

De esta manera, los términos de ISO 37001 forman parte de un único sistema de gestión orientado a **prevenir, detectar y responder ante el soborno**.

Aspectos clave para recordar

Para comprender correctamente ISO 37001, es importante recordar especialmente los siguientes conceptos:

- **Soborno:** oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida, de manera directa o indirecta, en las circunstancias contempladas por la norma y la legislación aplicable.
- **Riesgo de soborno:** posibilidad de que se produzca una situación de soborno que afecte a la organización.
- **Sistema de Gestión Antisoborno:** estructura organizada de políticas, procesos, controles y responsabilidades para gestionar el riesgo de soborno.
- **Socio de negocio:** parte externa con la que la organización mantiene o pretende establecer una relación empresarial.
- **Debida diligencia:** proceso de evaluación y análisis de información relevante para gestionar riesgos.
- **Controles financieros:** mecanismos destinados a reducir los riesgos de soborno relacionados con operaciones financieras.
- **Controles no financieros:** mecanismos aplicados a procesos como compras, contratación, selección y relaciones comerciales.
- **Función antisoborno:** función responsable de determinadas actividades de supervisión y gestión del sistema.
- **No conformidad:** incumplimiento de un requisito aplicable.
- **Acción correctiva:** medida destinada a eliminar la causa de una no conformidad y evitar su recurrencia.
- **Mejora continua:** proceso permanente mediante el cual la organización aumenta la eficacia de su Sistema de Gestión Antisoborno.

El dominio de estos términos permite al participante comprender con mayor precisión los siguientes contenidos del curso, especialmente los relacionados con **liderazgo, política antisoborno, función de cumplimiento, evaluación de riesgos, debida diligencia y controles operativos**.

2.4. Certificación de la organización vs. capacitación del personal

Introducción

Uno de los aspectos que suele generar mayor confusión al estudiar la **ISO 37001** es la diferencia entre la **certificación de un Sistema de Gestión Antisoborno** y la **capacitación de las personas en materia antisoborno**.

Ambos conceptos están relacionados, pero **no significan lo mismo y no producen el mismo tipo de reconocimiento**.

La **ISO 37001:2025** establece requisitos para que una organización pueda establecer, implementar, mantener y mejorar un **Sistema de Gestión Antisoborno (SGAS)**. La norma está dirigida a organizaciones de diferentes sectores, incluyendo organizaciones públicas, privadas y sin fines de lucro.

Por otro lado, una persona puede recibir **capacitación en ISO 37001, antisoborno, cumplimiento o gestión de riesgos**, adquiriendo conocimientos y competencias sobre estos temas. Esta capacitación no significa que la organización donde trabaja esté certificada bajo ISO 37001.

Comprender esta diferencia es fundamental para evitar afirmaciones incorrectas como **“tener un certificado de capacitación ISO 37001 significa que la empresa está certificada”**. Son situaciones completamente diferentes.

¿Qué significa certificar una organización?

La **certificación de una organización** significa que un organismo de certificación ha evaluado el Sistema de Gestión Antisoborno de esa organización frente a los requisitos establecidos por ISO 37001 y ha determinado su conformidad dentro de un **alcance definido**.

La certificación se refiere al **sistema de gestión de la organización**, no a que cada trabajador haya sido certificado individualmente.

El proceso de certificación evalúa aspectos como:

- El contexto de la organización.
- El liderazgo y compromiso de la dirección.
- La política antisoborno.
- La evaluación de riesgos.
- Los objetivos antisoborno.
- La función antisoborno.
- La competencia y capacitación.
- La debida diligencia.

- Los controles financieros y no financieros.
- Los canales de denuncia.
- La investigación de posibles incidentes.
- El seguimiento y medición.
- Las auditorías internas.
- La revisión por la dirección.
- Las acciones correctivas.
- La mejora continua.

En Perú, **INACAL acredita a organismos de certificación de sistemas de gestión** y reconoce dentro de los alcances de acreditación la certificación de sistemas basados en **ISO 37001 o NTP-ISO 37001**.

La certificación pertenece a la organización

Es importante comprender una regla básica:

La certificación ISO 37001 corresponde a la organización y al alcance certificado, no a una persona que haya realizado un curso.

Por ejemplo, una empresa minera puede implementar un Sistema de Gestión Antisoborno y posteriormente someterlo a un proceso de certificación.

Si el organismo de certificación determina que el sistema cumple los requisitos aplicables, puede emitir una certificación para el **alcance definido de esa organización**.

Esto no significa que todos sus trabajadores sean automáticamente “certificados en ISO 37001”.

De la misma manera, si un trabajador realiza un curso de 20 horas sobre ISO 37001, esto **no convierte a su empresa en una organización certificada**.

¿Qué es la capacitación del personal?

La **capacitación del personal** tiene como finalidad desarrollar los conocimientos, habilidades y competencias necesarias para que las personas puedan desempeñar adecuadamente sus funciones.

En un Sistema de Gestión Antisoborno, la organización debe determinar las competencias necesarias para las personas que realizan actividades que pueden afectar el desempeño del sistema.

La formación puede abordar temas como:

- Conceptos fundamentales de soborno.
- Política antisoborno.
- Riesgos de soborno.
- Identificación de situaciones sospechosas.
- Regalos y hospitalidad.
- Conflictos de interés.

- Debida diligencia.
- Controles financieros.
- Canales de denuncia.
- Procedimientos internos.
- Responsabilidades de los trabajadores.
- Consecuencias del incumplimiento.

La capacitación es, por tanto, **un componente del sistema**, pero no equivale por sí misma a la certificación del sistema.

Diferencia fundamental

La diferencia puede resumirse de la siguiente manera:

Certificación ISO 37001: evalúa el **Sistema de Gestión Antisoborno de una organización**.

Capacitación en ISO 37001: desarrolla los **conocimientos y competencias de una persona**.

Certificación de personas: cuando corresponda, evalúa formalmente la competencia de una persona de acuerdo con un esquema específico de certificación.

Son tres conceptos que no deben confundirse.

Ejemplo práctico

Supongamos que una empresa constructora decide implementar ISO 37001.

La empresa desarrolla su política antisoborno, realiza una evaluación de riesgos, establece controles, capacita a sus trabajadores, implementa procedimientos de debida diligencia y crea canales para comunicar posibles incidentes. Después de implementar el sistema, la organización puede solicitar una evaluación de certificación a un organismo de certificación competente.

Si el proceso es satisfactorio, la **organización puede obtener la certificación de su Sistema de Gestión Antisoborno dentro del alcance establecido**.

Ahora imaginemos que uno de sus trabajadores realiza un curso de 20 horas denominado “Bases de ISO 37001 y Cumplimiento Antisoborno”. El trabajador obtiene una constancia o certificado de participación en el curso.

Esto significa que:

El trabajador ha recibido capacitación.

La empresa puede utilizar esa capacitación como evidencia de formación o desarrollo de competencias, cuando corresponda.

Pero **el certificado del trabajador no demuestra que la empresa esté certificada bajo ISO 37001**.

La certificación no significa que todos los trabajadores sean expertos

Otro error frecuente consiste en pensar que una empresa certificada debe tener a todos sus trabajadores certificados individualmente en ISO 37001. Esto no es correcto. La organización debe determinar las **competencias necesarias** para las personas que realizan trabajos que afectan su desempeño y debe adoptar las medidas necesarias para que esas personas sean competentes.

La formación necesaria dependerá de las funciones y del nivel de exposición al riesgo. Por ejemplo, un trabajador que no participa en procesos de contratación puede necesitar una formación general sobre la política antisoborno.

En cambio, un trabajador encargado de compras puede necesitar conocimientos más específicos sobre:

- Evaluación de proveedores.
- Conflictos de interés.
- Debida diligencia.
- Regalos y hospitalidad.
- Controles de contratación.

Una persona que desempeña funciones relacionadas directamente con el sistema antisoborno puede necesitar una formación considerablemente más especializada. Por ello, **la capacitación debe guardar relación con las responsabilidades y riesgos de cada función**.

Capacitación general y capacitación especializada

No todas las capacitaciones dentro de una organización tienen necesariamente el mismo objetivo. La **capacitación general** puede estar dirigida a todo el personal y explicar los principios fundamentales de la política antisoborno.

Puede incluir:

- Qué es el soborno.
- Qué conductas están prohibidas.
- Cómo identificar situaciones de riesgo.
- Cómo comunicar una preocupación.
- Qué responsabilidades tiene cada trabajador.

La **capacitación especializada**, en cambio, puede estar dirigida a determinados grupos.

Por ejemplo:

Área de compras: evaluación de proveedores y controles de contratación.

Área financiera: controles de pagos, registros y transacciones.

Gerencia: liderazgo, responsabilidades y supervisión del sistema.

Función antisoborno: evaluación de riesgos, seguimiento, investigación y mejora del SGAS.

Esta diferenciación permite utilizar los recursos de capacitación de manera **proporcional al riesgo y a las responsabilidades**.

¿Qué demuestra un certificado de capacitación?

Un certificado o constancia de capacitación normalmente demuestra que una persona **participó o completó una determinada actividad formativa**, de acuerdo con las condiciones establecidas por el proveedor de capacitación.

Dependiendo del curso, también puede existir una evaluación de conocimientos.

En ese caso, la documentación puede indicar que el participante:

- Completó el programa.
- Cumplió con las horas establecidas.
- Participó en las actividades.
- Aprobó una evaluación, cuando corresponda.

Sin embargo, el significado exacto del documento depende de **quién lo emite, qué proceso de evaluación se realizó y qué esquema de certificación existe**.

Por ello, no debe utilizarse la expresión **"empresa certificada ISO 37001"** simplemente porque sus trabajadores hayan realizado cursos sobre la norma.

Capacitación, constancia y certificación de personas

También es necesario distinguir entre **capacitación** y **certificación de personas**. La capacitación busca desarrollar conocimientos y competencias.

La certificación de personas, en cambio, implica que un organismo de certificación evalúa la competencia de una persona frente a requisitos establecidos en un esquema de certificación.

En Perú, INACAL explica que los organismos de certificación de personas evalúan la capacidad de las personas para aplicar determinados conocimientos y habilidades definidos en un documento normativo. Estos organismos pueden acreditarse bajo la **NTP-ISO/IEC 17024**.

Por lo tanto:

Curso de capacitación: formación.

Constancia o certificado de curso: evidencia de la formación realizada, según las condiciones del programa.

Certificación de persona: evaluación formal de competencia bajo un esquema de certificación.

Certificación ISO 37001: evaluación del Sistema de Gestión Antisoborno de una organización.

¿Quién certifica un Sistema de Gestión Antisoborno?

La certificación del sistema debe ser realizada por un **organismo de certificación de sistemas de gestión** que tenga competencia y, cuando corresponda, acreditación para el alcance pertinente. El organismo de certificación realiza una evaluación independiente del sistema.

INACAL señala que los organismos de certificación de sistemas de gestión verifican que una entidad cumpla los requisitos establecidos en una norma técnica y que los organismos acreditados operan bajo los requisitos correspondientes para la auditoría y certificación de sistemas de gestión. Esto es diferente de una empresa que simplemente ofrece un curso sobre ISO 37001.

El papel de INACAL en Perú

En Perú, el **Instituto Nacional de Calidad (INACAL)** desempeña funciones relacionadas con la acreditación de organismos de evaluación de la conformidad. La acreditación constituye un reconocimiento formal de la **competencia técnica** de un organismo de evaluación de la conformidad después de una evaluación frente a normas y criterios aplicables.

Dentro de este sistema se encuentran los organismos de certificación de sistemas de gestión y los organismos de certificación de personas. INACAL reconoce actualmente dentro de los ámbitos correspondientes la **certificación de Sistemas de Gestión Antisoborno basada en ISO 37001**, así como la certificación de personas bajo el esquema correspondiente.

Certificación acreditada y certificación no acreditada

También es importante comprender la diferencia entre un organismo que está **acreditado** para un determinado alcance y uno que no lo está. La acreditación significa que el organismo de evaluación de la conformidad ha demostrado su competencia frente a los requisitos establecidos por el organismo de acreditación correspondiente.

En Perú, INACAL administra el sistema nacional de acreditación y mantiene información sobre los organismos de certificación acreditados y sus respectivos alcances. Por esta razón, una organización que esté considerando certificarse debe revisar cuidadosamente:

- Quién realizará la certificación.
- Qué norma será utilizada.
- Qué alcance tiene la certificación.
- Si el organismo tiene competencia para ese alcance.

- Qué esquema de acreditación corresponde.
- Qué actividades serán evaluadas.

El alcance de la certificación

La certificación ISO 37001 no debe interpretarse como una afirmación ilimitada sobre todas las actividades posibles de una organización. La certificación se relaciona con un **alcance determinado**.

El alcance puede especificar las actividades, procesos, unidades organizativas, ubicaciones u otras condiciones que forman parte del Sistema de Gestión Antisoborno evaluado. Esto es especialmente importante para organizaciones grandes que desarrollan muchas actividades diferentes.

Por ejemplo, una organización puede tener operaciones administrativas, comerciales, industriales y de contratación pública. El alcance certificado debe indicar claramente **qué actividades y unidades están incluidas**.

INACAL establece que la acreditación de organismos de certificación de sistemas de gestión considera, entre otros elementos, el documento normativo y los sectores de actividad correspondientes. ISO 37001 se encuentra expresamente incluida entre las normas para las cuales puede acreditarse la certificación de sistemas de gestión.

La capacitación como parte del Sistema de Gestión Antisoborno

Aunque la capacitación no equivale a la certificación, desempeña un papel importante dentro de ISO 37001. Una organización no puede depender únicamente de políticas escritas. Las personas que participan en procesos relevantes deben **conocer sus responsabilidades y comprender los riesgos relacionados con sus funciones**.

Por ello, la capacitación puede contribuir a:

- Crear conciencia sobre el soborno.
- Explicar la política antisoborno.
- Desarrollar competencias.
- Reducir errores.
- Mejorar la identificación de riesgos.
- Fortalecer los controles.
- Facilitar la comunicación de incidentes.
- Promover una cultura de integridad.

La capacitación es, por tanto, **una herramienta para hacer que el sistema funcione en la práctica**.

Evidencia de la capacitación

Una organización debe conservar evidencia apropiada de las actividades de formación realizadas cuando ello sea necesario para demostrar el cumplimiento de sus requisitos internos y del sistema.

Entre las evidencias pueden encontrarse:

- Listas de participantes.
- Certificados o constancias.
- Programas de capacitación.
- Materiales utilizados.
- Evaluaciones.
- Resultados obtenidos.
- Fechas de capacitación.
- Registros de asistencia.
- Identificación del personal capacitado.

Estas evidencias pueden resultar útiles durante auditorías internas o evaluaciones externas. Sin embargo, nuevamente debe recordarse que **la existencia de certificados de capacitación no sustituye la implementación del Sistema de Gestión Antisoborno**.

¿Puede una empresa estar certificada sin capacitar a absolutamente todos?

La respuesta debe analizarse desde los requisitos de competencia y concienciación aplicables al sistema. La certificación de la organización no significa necesariamente que cada persona que trabaja en ella haya realizado un curso externo denominado “ISO 37001”.

Lo relevante es que la organización haya determinado las **competencias y conocimientos necesarios** para las funciones pertinentes y haya implementado medidas adecuadas para garantizar que las personas sean competentes y conscientes de sus responsabilidades.

Esto puede lograrse mediante diferentes mecanismos:

- Capacitación interna.
- Cursos externos.
- Talleres.
- Entrenamiento en el puesto.
- Sesiones de sensibilización.
- Instrucciones específicas.
- Evaluaciones de conocimiento.
- Experiencia profesional.
- Otros métodos apropiados.

Por ello, **ISO 37001 no debe interpretarse como una obligación de que todos los trabajadores posean un certificado externo individual**.

¿Puede una persona capacitada implementar ISO 37001?

Una persona que haya recibido capacitación puede adquirir conocimientos útiles para participar en la implementación del sistema. Sin embargo, **realizar un curso no garantiza por sí solo que una persona tenga todas las competencias necesarias para implementar o administrar un Sistema de Gestión Antisoborno**.

La implementación puede requerir conocimientos adicionales sobre:

- Gestión de riesgos.
- Procesos organizacionales.
- Legislación aplicable.
- Auditoría.
- Controles internos.
- Cumplimiento.
- Gestión documental.
- Investigación.
- Gobierno corporativo.

Las competencias necesarias dependerán de las responsabilidades asignadas a la persona.

¿Puede una empresa capacitar a sus trabajadores sin certificarse?

Sí. Una organización puede implementar programas de capacitación antisoborno incluso si todavía **no busca obtener una certificación ISO 37001**. De hecho, la capacitación puede utilizarse como parte de una estrategia de prevención y cumplimiento.

Una empresa puede comenzar por:

Capacitar al personal → identificar riesgos → establecer controles → desarrollar procedimientos → evaluar resultados → mejorar progresivamente el sistema.

Posteriormente, si la dirección decide obtener una certificación, la organización puede someter su sistema a una evaluación externa.

¿Puede una empresa certificarse sin tener capacitación?

La capacitación y la competencia forman parte de los elementos relevantes del sistema, por lo que una organización que pretenda demostrar conformidad con ISO 37001 debe gestionar adecuadamente las **competencias y concienciación necesarias**.

Por tanto, no sería correcto pensar que una organización puede simplemente crear documentos y obtener una certificación sin demostrar que las personas relevantes conocen y pueden cumplir sus responsabilidades.

La certificación evalúa el **sistema en funcionamiento**, no solamente la existencia de documentos.

Diferencia entre “certificado ISO 37001” y “certificado de capacitación ISO 37001”

Esta distinción debe quedar absolutamente clara. Cuando se habla de un **certificado ISO 37001 de una organización**, normalmente se está haciendo referencia a la certificación de un Sistema de Gestión Antisoborno conforme a ISO 37001, dentro de un alcance determinado.

Cuando se habla de un **certificado de capacitación en ISO 37001**, se está haciendo referencia a un documento que acredita la participación o aprobación de una persona en un programa formativo, según las características de dicho programa.

Por lo tanto, las siguientes afirmaciones **no son equivalentes**:

“La empresa está certificada bajo ISO 37001.” Y **“El trabajador tiene un certificado de capacitación en ISO 37001.”** La primera se refiere a una **organización y su sistema de gestión**. La segunda se refiere a una **persona y su formación**.

Ejemplo aplicado al sector minero

Una empresa minera peruana puede implementar un Sistema de Gestión Antisoborno debido a los riesgos asociados con proveedores, contratistas, permisos, relaciones con autoridades, adquisiciones y otros procesos.

La empresa puede capacitar a:

- Personal administrativo.
- Personal de compras.
- Personal financiero.
- Supervisores.
- Gerentes.
- Personal encargado de cumplimiento.

Cada grupo puede recibir formación adaptada a sus responsabilidades. Posteriormente, la empresa puede realizar auditorías internas y mejorar sus controles.

Si la organización decide obtener la certificación ISO 37001, deberá someter su **Sistema de Gestión Antisoborno** a la evaluación correspondiente por un organismo de certificación competente. Los certificados de capacitación de sus trabajadores pueden constituir **evidencia de formación**, pero no sustituyen la certificación del sistema.

Ejemplo aplicado a una municipalidad

Una entidad pública también puede desarrollar capacidades internas relacionadas con la prevención del soborno.

Puede capacitar a funcionarios y servidores sobre:

- Riesgos en contrataciones.
- Conflictos de interés.
- Regalos y hospitalidad.
- Relaciones con proveedores.
- Canales de denuncia.
- Responsabilidades individuales.
- Política antisoborno.

Si posteriormente la entidad implementa un Sistema de Gestión Antisoborno conforme a ISO 37001 y busca certificarse, la evaluación se realizará sobre el **sistema de gestión de la organización**, no sobre los certificados individuales de los trabajadores.

La importancia de comunicar correctamente

Utilizar correctamente los términos relacionados con certificación y capacitación es especialmente importante para mantener la **transparencia y credibilidad**. Una institución educativa puede afirmar correctamente:

“Curso de capacitación en fundamentos de ISO 37001 y cumplimiento antisoborno.”

Puede emitir una constancia o certificado de capacitación de acuerdo con las condiciones del programa.

Lo que no debe hacer, salvo que exista realmente el reconocimiento o proceso correspondiente, es presentar esa capacitación como si otorgara una **certificación ISO 37001 a la empresa del participante**.

Del mismo modo, una organización certificada debe comunicar claramente **qué ha sido certificado y cuál es el alcance de la certificación**.

Certificación y mejora continua

La certificación tampoco significa que una organización haya alcanzado un estado permanente de perfección. ISO 37001:2025 está concebida como un **sistema de gestión que debe mantenerse y mejorarse continuamente**.

Por ello, una organización certificada debe continuar trabajando en aspectos como:

- Evaluación de riesgos.
- Controles.
- Capacitación.
- Auditorías.
- Seguimiento.
- Investigación de incidentes.
- Acciones correctivas.
- Revisión por la dirección.
- Mejora continua.

La certificación representa una evaluación de conformidad del sistema dentro de un determinado alcance y bajo las condiciones correspondientes; **no significa que el riesgo de soborno haya desaparecido**.

Relación entre certificación y capacitación

La relación correcta puede representarse de la siguiente manera:

Capacitación del personal

↓

Desarrollo de conocimientos y competencias

↓

Implementación del Sistema de Gestión Antisoborno

↓

Aplicación de políticas, controles y procedimientos

↓

Evaluación del sistema

↓

Auditoría y revisión

↓

Certificación de la organización, cuando la organización decide someterse al proceso y cumple los requisitos aplicables.

Esta relación demuestra que la capacitación puede ser **una parte importante del camino hacia un sistema eficaz**, pero no es equivalente a la certificación.

Aspectos clave para recordar

La **certificación ISO 37001 y la capacitación en ISO 37001 son conceptos diferentes**. La certificación ISO 37001 se refiere al **Sistema de Gestión Antisoborno de una organización** y se realiza mediante un proceso de evaluación llevado a cabo por un organismo de certificación competente.

La capacitación se refiere al **desarrollo de conocimientos y competencias de las personas**. Un certificado de capacitación **no convierte a una empresa en una organización certificada bajo ISO 37001**.

Una organización certificada no necesita que absolutamente todos sus trabajadores posean un certificado externo individual de ISO 37001, pero sí debe gestionar adecuadamente las **competencias, concienciación y formación necesarias para las funciones relevantes**.

En Perú, es importante distinguir además entre los organismos que **certifican sistemas de gestión** y los organismos que **certifican personas**, ya que se trata de procesos de evaluación de la conformidad diferentes. INACAL mantiene esquemas y directorios diferenciados para ambos tipos de organismos.

Finalmente, debe recordarse que **ISO 37001:2025 certifica sistemas de gestión, no "certifica" automáticamente a las personas que trabajan dentro de la organización**. La capacitación del personal es un elemento que contribuye al funcionamiento del sistema; la

certificación, en cambio, es el resultado de una evaluación formal de conformidad del sistema de gestión dentro de un alcance determinado.

2.5. Relación con otras normas ISO

Introducción

La **ISO 37001:2025** forma parte de una familia más amplia de normas ISO orientadas a mejorar la gestión de las organizaciones. Aunque su objetivo específico es la **prevención, detección y respuesta frente al soborno**, su estructura permite relacionarla e integrarla con otros sistemas de gestión.

ISO señala expresamente que ISO 37001 puede implementarse como un sistema independiente o **integrarse dentro de un marco de gestión existente**, complementando otros sistemas y directrices relacionados con el cumplimiento, la ética y la gobernanza.

Esta posibilidad es especialmente importante para organizaciones que ya cuentan con sistemas de gestión de **calidad, medio ambiente, seguridad y salud en el trabajo, compliance, seguridad de la información u otras áreas**.

La integración permite evitar la creación de sistemas completamente separados y facilita el uso de procesos comunes, como la gestión de riesgos, auditorías, documentación, capacitación, objetivos y mejora continua.

ISO 37001 dentro de los sistemas de gestión

La ISO 37001:2025 es una norma de **sistema de gestión antisoborno**. Su finalidad específica es ayudar a la organización a establecer, implementar, mantener y mejorar un sistema destinado a gestionar los riesgos relacionados con el soborno.

El sistema incluye elementos como:

- Política antisoborno.
- Liderazgo y compromiso de la dirección.
- Evaluación de riesgos.
- Objetivos.
- Función antisoborno.
- Debida diligencia.
- Controles financieros.
- Controles no financieros.
- Capacitación.
- Comunicación.
- Canales de denuncia.
- Investigación.
- Seguimiento y medición.
- Auditoría interna.
- Revisión por la dirección.
- Acciones correctivas.
- Mejora continua.

Por tanto, **ISO 37001 no debe entenderse como una norma aislada de los demás procesos de gestión de una organización**.

La prevención del soborno puede estar directamente relacionada con la forma en que una empresa compra, contrata, vende, gestiona proveedores, administra sus recursos, protege información y cumple sus obligaciones legales.

La estructura común de las normas ISO

Una de las principales razones por las que diferentes normas ISO pueden integrarse es que muchas normas de sistemas de gestión utilizan una **estructura armonizada común**.

Esta estructura facilita que determinados elementos puedan gestionarse de manera conjunta.

Entre los elementos que suelen compartir se encuentran:

- Contexto de la organización.
- Liderazgo.
- Planificación.
- Recursos y apoyo.
- Operación.
- Evaluación del desempeño.
- Mejora.

La ISO 37001 también está diseñada para facilitar su integración con otros sistemas de gestión. El comité técnico de ISO indica que la norma sigue una estructura común de las normas de sistemas de gestión, lo que facilita su integración con otros sistemas.

Esto significa que una organización no necesariamente necesita crear **seis sistemas administrativos completamente independientes** para gestionar calidad, medio ambiente, seguridad, compliance y antisoborno.

Puede desarrollar un **sistema de gestión integrado**, manteniendo los requisitos específicos de cada norma.

ISO 37001 e ISO 37301

Una de las relaciones más importantes es la existente entre:

ISO 37001:2025 — Sistema de Gestión Antisoborno y **ISO 37301:2021 — Sistema de Gestión del Compliance.**

ISO 37301 establece requisitos y orientación para desarrollar, implementar, evaluar, mantener y mejorar un **Sistema de Gestión del Compliance**.

Mientras que ISO 37001 se concentra específicamente en el **soborno**, ISO 37301 tiene un alcance más amplio y aborda la gestión del cumplimiento de leyes, reglamentos, requisitos y compromisos aplicables a la organización.

Por ello, puede entenderse la relación de la siguiente manera:

ISO 37301 = enfoque amplio de compliance.

ISO 37001 = enfoque específico en antisoborno.

ISO 37001 dentro de un sistema de compliance

Una organización puede utilizar ISO 37301 como marco general para su sistema de compliance y utilizar ISO 37001 para desarrollar controles más específicos relacionados con el soborno.

Por ejemplo, un sistema de compliance puede gestionar riesgos relacionados con:

- Legislación laboral.
- Protección de datos.
- Obligaciones tributarias.
- Regulaciones sectoriales.
- Competencia.
- Contratos.
- Requisitos ambientales.
- Antisoborno.

Dentro de este sistema más amplio, **ISO 37001 proporciona un marco especializado para gestionar los riesgos de soborno**.

Esto resulta especialmente útil en organizaciones grandes que necesitan gestionar simultáneamente diferentes categorías de obligaciones.

ISO 37001 e ISO 9001

La **ISO 9001** establece requisitos para un **Sistema de Gestión de la Calidad**.

Su objetivo principal es ayudar a las organizaciones a gestionar sus procesos para proporcionar productos y servicios que cumplan los requisitos aplicables y mejorar la satisfacción del cliente.

ISO 37001 tiene un objetivo diferente: **gestionar los riesgos relacionados con el soborno**.

Sin embargo, ambas pueden integrarse.

Por ejemplo, una empresa que ya dispone de ISO 9001 puede aprovechar procesos existentes de:

- Control documental.
- Gestión de procesos.
- Evaluación de proveedores.
- Gestión de riesgos.
- Auditoría interna.

- Seguimiento de indicadores.
- Acciones correctivas.
- Mejora continua.

Sobre esta estructura puede incorporar los requisitos específicos de ISO 37001.

Ejemplo de integración con ISO 9001

Supongamos que una empresa ya tiene un procedimiento para **evaluar y seleccionar proveedores** dentro de su Sistema de Gestión de la Calidad.

Cuando implementa ISO 37001, puede utilizar ese mismo proceso como punto de partida para incorporar elementos de **debida diligencia antisoborno**.

El proceso podría incorporar preguntas adicionales relacionadas con:

- Riesgo de soborno.
- Conflictos de interés.
- Relaciones con funcionarios públicos.
- Antecedentes relevantes.
- Beneficiarios finales, cuando corresponda.
- Riesgo asociado al tipo de servicio.

De esta manera, la organización no necesita necesariamente crear un proceso completamente separado.

El proceso de proveedores puede cumplir simultáneamente objetivos de calidad y objetivos antisoborno, siempre que se incorporen y gestionen adecuadamente los requisitos específicos de cada sistema.

ISO 37001 e ISO 14001

La **ISO 14001** establece los requisitos para los Sistemas de Gestión Ambiental.

Su finalidad es ayudar a las organizaciones a gestionar sus aspectos ambientales y mejorar su desempeño ambiental.

Aunque el medio ambiente y el antisoborno son materias diferentes, ambas normas pueden compartir determinados procesos de gestión.

Por ejemplo:

- Identificación del contexto.
- Evaluación de riesgos.
- Gestión de documentación.
- Competencia y capacitación.
- Comunicación.
- Auditoría interna.
- Revisión por la dirección.
- Acciones correctivas.

- Mejora continua.

Una empresa minera, industrial o constructora puede tener simultáneamente **ISO 14001 e ISO 37001**, utilizando una estructura administrativa común.

Ejemplo en una empresa minera

Una empresa minera puede tener riesgos ambientales relacionados con sus operaciones y, simultáneamente, riesgos de soborno relacionados con:

- Contratación de proveedores.
- Contratistas.
- Permisos.
- Inspecciones.
- Relaciones con autoridades.
- Adquisiciones.
- Servicios especializados.

La organización puede gestionar los riesgos ambientales mediante ISO 14001 y los riesgos de soborno mediante ISO 37001.

Los dos sistemas pueden compartir procesos como:

Gestión documental → capacitación → auditoría → revisión por la dirección → acciones correctivas → mejora continua.

Sin embargo, **los objetivos y controles específicos permanecen diferenciados**.

ISO 37001 e ISO 45001

La **ISO 45001** establece requisitos para los Sistemas de Gestión de Seguridad y Salud en el Trabajo.

Esta norma está orientada a gestionar riesgos relacionados con la seguridad y salud de los trabajadores. ISO 37001, por su parte, se concentra en los riesgos de soborno.

Aunque sus materias son diferentes, una organización puede utilizar estructuras comunes de gestión. Por ejemplo, una empresa de construcción podría tener:

ISO 45001 para gestionar riesgos de accidentes y condiciones de trabajo.

ISO 37001 para gestionar riesgos de soborno relacionados con contrataciones, proveedores, intermediarios y relaciones con entidades públicas.

Ambos sistemas pueden compartir:

- Procesos de capacitación.
- Auditorías internas.
- Gestión documental.
- Objetivos.

- Seguimiento.
- Revisión por la dirección.
- Acciones correctivas.

ISO 37001 e ISO 27001

La **ISO/IEC 27001** establece requisitos para un **Sistema de Gestión de Seguridad de la Información**. Su objetivo es gestionar los riesgos relacionados con la seguridad de la información.

En determinadas organizaciones puede existir una relación práctica entre seguridad de la información y antisoborno.

Por ejemplo, los registros relacionados con:

- Denuncias.
- Investigaciones.
- Evaluaciones de terceros.
- Información financiera.
- Contratos.
- Datos de proveedores.

pueden contener información sensible que necesita ser protegida.

Por ello, una organización que dispone de ISO 27001 puede utilizar determinados controles de seguridad de la información para proteger la **confidencialidad, integridad y disponibilidad de información relacionada con su Sistema de Gestión Antisoborno**.

Sin embargo, ISO 27001 no sustituye a ISO 37001. **Una norma gestiona riesgos de seguridad de la información y la otra gestiona riesgos de soborno.**

ISO 37002 y los canales de denuncia

Existe además una relación especialmente interesante con la **ISO 37002:2021**, denominada Whistleblowing management systems — Guidelines.

Esta norma proporciona directrices para establecer sistemas de gestión de denuncias y está específicamente relacionada con la gestión de información recibida mediante mecanismos de whistleblowing.

ISO 37001 incluye mecanismos para **reportar preocupaciones y gestionar posibles incidentes de soborno**, mientras que ISO 37002 proporciona un marco específico para gestionar sistemas de denuncia. Por ello, una organización puede considerar ambas normas de manera complementaria.

ISO 37001 e ISO 37002: diferencia

Es importante no confundirlas.

ISO 37001 tiene como objeto principal el **Sistema de Gestión Antisoborno**.

ISO 37002 se concentra en el **Sistema de Gestión de Denuncias**.

Una organización puede implementar ISO 37001 sin implementar ISO 37002.

También puede utilizar principios y buenas prácticas de ISO 37002 para fortalecer el mecanismo de denuncias de su Sistema de Gestión Antisoborno.

ISO 37001 e ISO 37003

La familia de normas relacionada con integridad y gobernanza también incluye **ISO 37003:2025**, orientada a proporcionar directrices para organizaciones que gestionan el riesgo de fraude.

Esto es relevante porque **fraude y soborno no son conceptos idénticos**, aunque pueden aparecer relacionados en determinadas situaciones.

ISO 37001 se centra en el soborno.

ISO 37003 proporciona orientación sobre la gestión del riesgo de fraude.

La existencia de estas normas permite a una organización desarrollar enfoques complementarios para diferentes categorías de riesgo.

ISO 37001 y gestión del riesgo

La gestión de riesgos constituye otro punto de conexión entre ISO 37001 y otros sistemas de gestión. Una organización puede utilizar una metodología corporativa común para identificar, analizar, evaluar y tratar diferentes tipos de riesgos.

Por ejemplo, una matriz corporativa podría incluir:

- Riesgos financieros.
- Riesgos operacionales.
- Riesgos legales.
- Riesgos ambientales.
- Riesgos de seguridad y salud.
- Riesgos de seguridad de la información.
- **Riesgos de soborno.**

Sin embargo, debe evitarse un error importante:

Utilizar una metodología común no significa que todos los riesgos sean iguales.

Los riesgos de soborno tienen características específicas y deben evaluarse considerando las circunstancias propias de la organización y sus relaciones.

Integración de sistemas de gestión

Una organización que posee varios sistemas ISO puede desarrollar un **Sistema Integrado de Gestión (SIG)**.

Por ejemplo, una empresa podría integrar:

ISO 9001 — Calidad.

ISO 14001 — Medio ambiente.

ISO 45001 — Seguridad y salud en el trabajo.

ISO 37001 — Antisoborno.

ISO 37301 — Compliance.

ISO/IEC 27001 — Seguridad de la información.

La organización puede mantener procedimientos comunes cuando resulte apropiado y, al mismo tiempo, mantener los controles específicos de cada disciplina.

Ventajas de la integración

La integración puede generar diferentes beneficios.

Entre ellos:

- **Evitar duplicación de procesos.**
- Reducir documentos innecesarios.
- Simplificar determinadas auditorías.
- Utilizar una metodología común de gestión de riesgos.
- Coordinar mejor las responsabilidades.
- Facilitar la capacitación.
- Centralizar determinados registros.
- Mejorar el seguimiento de objetivos.
- Facilitar la revisión por la dirección.
- Fortalecer la visión global de los riesgos.

La propia ISO indica que ISO 37001 puede integrarse con sistemas de gestión existentes y que sus medidas están diseñadas para integrarse con procesos y controles ya existentes.

Lo que no debe hacerse al integrar normas

La integración no significa simplemente colocar diferentes logotipos o nombres de normas dentro del mismo manual. Un sistema integrado debe **cumplir los requisitos específicos de cada norma aplicable**.

Por ejemplo, una empresa puede utilizar un único procedimiento de auditoría interna para diferentes sistemas.

Pero durante la auditoría deben evaluarse los requisitos correspondientes a cada norma. De igual manera, un único proceso de gestión de proveedores puede utilizarse para ISO 9001 e ISO 37001, pero debe incorporar **los criterios específicos de calidad y los controles antisoborno que correspondan**.

Un procedimiento puede servir para varias normas

Este es uno de los conceptos más importantes de la integración. Un mismo proceso organizacional puede tener diferentes objetivos de control. Por ejemplo, un procedimiento de contratación de proveedores puede incluir:

ISO 9001: criterios relacionados con la capacidad del proveedor y la calidad.

ISO 14001: criterios ambientales cuando sean relevantes.

ISO 45001: criterios de seguridad y salud.

ISO 37001: criterios de riesgo de soborno y debida diligencia.

ISO 37301: requisitos de compliance aplicables.

Esto permite construir procesos más completos sin necesariamente crear procedimientos completamente separados.

Ejemplo de proceso integrado de compras

Supongamos que una empresa necesita contratar a un nuevo proveedor.

El proceso integrado podría comenzar con la identificación de la necesidad y continuar con la evaluación del proveedor.

Desde el punto de vista de **ISO 9001**, se podría evaluar su capacidad para cumplir los requisitos de calidad.

Desde **ISO 14001**, podrían evaluarse determinados aspectos ambientales.

Desde **ISO 45001**, podrían considerarse aspectos de seguridad y salud cuando sean pertinentes.

Desde **ISO 37001**, se podría realizar una **debida diligencia basada en el riesgo de soborno**.

Desde **ISO 37301**, podrían revisarse determinadas obligaciones de compliance aplicables.

El resultado sería un proceso de contratación **más completo y coordinado**.

Integración con la gobernanza corporativa

ISO 37001 también puede relacionarse con la **gobernanza de la organización**. La prevención del soborno no corresponde únicamente al área de cumplimiento.

Puede involucrar:

- Alta dirección.
- Directorio o máximo órgano de gobierno, cuando corresponda.
- Finanzas.
- Compras.
- Recursos humanos.
- Área legal.
- Auditoría interna.
- Operaciones.
- Gestión de riesgos.
- Compliance.

Cuando ISO 37001 se integra con otros sistemas, puede contribuir a una visión más amplia de **gobernanza, riesgo y cumplimiento**.

La relación entre ISO 37001 e ISO 37301 es especialmente importante

Para este curso, debe prestarse especial atención a la relación entre estas dos normas.

ISO 37001 se concentra en un riesgo específico: **el soborno**.

ISO 37301 proporciona un sistema de gestión más amplio para el **cumplimiento**.

Esto significa que una organización puede utilizar ISO 37301 para estructurar su sistema general de compliance y utilizar ISO 37001 para profundizar específicamente en la prevención, detección y respuesta frente al soborno. ISO confirma expresamente que ISO 37301 puede integrarse con ISO 37001, así como con otras normas de sistemas de gestión como ISO 9001 e ISO 14001.

No todas las normas tienen el mismo propósito

Es fundamental no pensar que todas las normas ISO son intercambiables.

Cada una tiene un **objeto y alcance específico**.

Por ejemplo:

ISO 9001: calidad.

ISO 14001: gestión ambiental.

ISO 45001: seguridad y salud en el trabajo.

ISO/IEC 27001: seguridad de la información.

ISO 37301: compliance.

ISO 37001: antisoborno.

ISO 37002: gestión de denuncias.

ISO 37003: gestión del riesgo de fraude.

Una organización puede integrarlas, pero **una norma no sustituye automáticamente a otra**.

ISO 37001 y el cumplimiento legal

ISO 37001 también tiene una relación importante con el cumplimiento de las leyes y regulaciones aplicables. La norma no reemplaza la legislación nacional.

Una organización que implementa ISO 37001 debe considerar las **obligaciones legales y regulatorias aplicables a sus actividades**.

En el caso de una organización que opera en Perú, esto significa que el sistema antisoborno debe desarrollarse teniendo en cuenta el marco jurídico peruano correspondiente, además de los compromisos internacionales y contractuales que resulten aplicables.

Por tanto:

ISO 37001 proporciona un marco de gestión.

La legislación establece obligaciones jurídicas.

La organización debe gestionar ambos elementos de manera coherente.

ISO 37001 como parte de una estrategia integral

Una organización madura puede utilizar ISO 37001 como una pieza de una estrategia más amplia de:

- Integridad.
- Ética.
- Compliance.
- Gestión de riesgos.
- Gobierno corporativo.
- Transparencia.
- Control interno.

Esto permite pasar de una visión limitada de **“cumplir una norma”** a una visión más completa de **gestionar los riesgos que pueden afectar a la organización**.

Ejemplo de una organización con varios sistemas

Imaginemos una empresa de construcción que trabaja en proyectos privados y contrataciones con entidades públicas.

La organización podría utilizar:

ISO 9001 para gestionar la calidad de sus proyectos.

ISO 14001 para gestionar sus aspectos ambientales.

ISO 45001 para gestionar la seguridad y salud de sus trabajadores.

ISO 37001 para gestionar los riesgos de soborno.

ISO 37301 para establecer un sistema general de compliance.

En este escenario, la organización podría tener una estructura común para:

- Gestión documental.
- Auditoría.
- Gestión de riesgos.
- Capacitación.
- Seguimiento de indicadores.
- Acciones correctivas.
- Revisión por la dirección.

Al mismo tiempo, cada norma mantendría sus **requisitos y objetivos específicos**.

El enfoque basado en procesos

La integración funciona mejor cuando la organización piensa en términos de **procesos reales** y no solamente en términos de normas.

En lugar de preguntar:

“¿Qué documento necesita ISO 37001?”

es más útil preguntar:

“¿Cómo funciona actualmente nuestro proceso de compras y qué riesgos de soborno existen dentro de él?”

Después se pueden incorporar los controles necesarios.

Este enfoque permite que ISO 37001 se integre en las operaciones reales de la organización y no se convierta simplemente en un conjunto adicional de documentos.

El enfoque basado en riesgos

La integración también debe considerar el **nivel de riesgo**. No todos los procesos necesitan el mismo nivel de control antisoborno. Por ejemplo, un pequeño proveedor de material de oficina puede presentar un nivel de riesgo diferente al de un intermediario que representa a la organización frente a autoridades públicas.

Por ello, los controles de ISO 37001 deben aplicarse de manera **proporcional al riesgo**.

Este principio permite integrar la norma sin crear una carga administrativa innecesaria.

Integración y auditoría

Cuando existen varios sistemas de gestión, las auditorías también pueden coordinarse. Una organización puede realizar una auditoría integrada en la que se revisen simultáneamente determinados procesos frente a varios criterios.

Por ejemplo, durante una auditoría del proceso de compras se pueden revisar:

- Requisitos de calidad.
- Criterios ambientales.
- Seguridad y salud.
- Controles antisoborno.
- Requisitos de compliance.

Esto puede mejorar la eficiencia de las auditorías, siempre que los auditores tengan las **competencias necesarias para evaluar los requisitos correspondientes**.

Integración y mejora continua

La integración de sistemas también puede fortalecer la **mejora continua**. Una no conformidad detectada en un proceso puede tener implicaciones para diferentes áreas.

Por ejemplo, una deficiencia en la gestión de proveedores puede revelar simultáneamente:

- Un problema de calidad.
- Un riesgo ambiental.
- Un riesgo de seguridad.
- Un riesgo de soborno.
- Un incumplimiento de compliance.

Una visión integrada permite analizar el problema de manera más completa y desarrollar acciones correctivas coordinadas.

Aspectos clave para recordar

La **ISO 37001:2025 puede implementarse de forma independiente o integrarse con otros sistemas de gestión**.

La relación más directa se produce con **ISO 37301**, porque ambas están relacionadas con el ámbito del compliance, aunque tienen alcances diferentes: ISO 37001 se concentra en el **soborno**, mientras ISO 37301 aborda el **cumplimiento de manera más amplia**.

También puede integrarse con sistemas como:

- **ISO 9001:** gestión de la calidad.
- **ISO 14001:** gestión ambiental.
- **ISO 45001:** seguridad y salud en el trabajo.
- **ISO/IEC 27001:** seguridad de la información.
- **ISO 37002:** gestión de denuncias.
- **ISO 37003:** gestión del riesgo de fraude.

La integración permite compartir determinados procesos y recursos, pero **no elimina los requisitos específicos de cada norma**.

El objetivo final no es acumular certificados, procedimientos o documentos, sino construir un sistema de gestión que permita a la organización **gestionar sus riesgos de manera coordinada, proporcional y eficaz**.

En el caso de ISO 37001, esto significa integrar la prevención del soborno dentro de las actividades reales de la organización, de manera que la **integridad, el cumplimiento y la gestión de riesgos formen parte de la toma de decisiones y de las operaciones cotidianas**.

3. Liderazgo y Política Antisoborno

3.1. Rol de la alta dirección

Introducción

En un Sistema de Gestión Antisoborno, el compromiso de la **alta dirección** es uno de los elementos fundamentales para que el sistema funcione de manera efectiva. ISO 37001:2025 establece requisitos específicos de liderazgo y compromiso, incluyendo la responsabilidad de establecer la política y los objetivos antisoborno, proporcionar recursos, integrar el sistema en los procesos de negocio y promover una cultura antisoborno.

La prevención del soborno no debe considerarse únicamente una responsabilidad del área legal, de auditoría o de cumplimiento. **La dirección debe asumir un papel activo y visible**, demostrando mediante sus decisiones y comportamientos que la organización no tolera prácticas de soborno.

¿Qué se entiende por alta dirección?

La **alta dirección** está constituida por la persona o grupo de personas que dirige y controla la organización al más alto nivel.

Dependiendo de la estructura de la organización, puede tratarse de:

- Gerente general.
- Director ejecutivo.
- Gerentes de alto nivel.
- Administradores con autoridad máxima.
- Máximo responsable de una determinada unidad incluida dentro del alcance del sistema.

En organizaciones que cuentan con un **órgano de gobierno separado**, como un directorio o consejo, también existen responsabilidades específicas para dicho órgano. En

organizaciones pequeñas, es posible que **la alta dirección y el órgano de gobierno recaigan en las mismas personas**. ISO 37001:2025 contempla esta posibilidad.

Compromiso visible de la dirección

La alta dirección no debe limitarse a aprobar documentos. Debe demostrar mediante sus acciones que la prevención del soborno constituye una prioridad de la organización.

Este compromiso puede manifestarse mediante:

- Aprobación de la política antisoborno.
- Establecimiento de objetivos antisoborno.
- Asignación de recursos.
- Participación en actividades de sensibilización.
- Comunicación de la importancia del cumplimiento.
- Supervisión del funcionamiento del sistema.
- Apoyo a la función antisoborno.
- Promoción de una cultura de integridad.
- Rechazo de comportamientos incompatibles con la política antisoborno.

Lo que la dirección hace en la práctica debe ser coherente con lo que establece la política antisoborno.

Integración del antisoborno en la gestión

Uno de los aspectos importantes de ISO 37001:2025 es que los requisitos del Sistema de Gestión Antisoborno deben integrarse en los **procesos de negocio de la organización**. Esto significa que la prevención del soborno no debe funcionar como una actividad completamente separada de las operaciones.

Por ejemplo, puede incorporarse en:

- Procesos de compras.
- Contratación de proveedores.
- Gestión de intermediarios.
- Ventas.
- Contrataciones con entidades públicas.
- Gestión financiera.
- Recursos humanos.
- Proyectos.
- Relaciones con socios comerciales.

De esta manera, **el antisoborno se convierte en parte de la forma habitual de gestionar la organización**.

Asignación de recursos

La alta dirección debe asegurar que existan **recursos adecuados y necesarios** para que el Sistema de Gestión Antisoborno pueda funcionar.

Estos recursos pueden incluir:

- Personal competente.
- Tiempo de trabajo.
- Presupuesto.
- Capacitación.
- Herramientas tecnológicas.
- Recursos para auditorías.
- Recursos para investigaciones.
- Sistemas de comunicación y denuncia.

No sería coherente que una organización declare que la prevención del soborno es una prioridad y, al mismo tiempo, no proporcione los medios necesarios para implementar sus controles.

Promoción de una cultura antisoborno

La edición **ISO 37001:2025 incorpora expresamente el requisito de desarrollar, mantener y promover una cultura antisoborno en todos los niveles de la organización**.

La alta dirección y los responsables de la organización deben demostrar un compromiso **activo, visible, coherente y sostenido** con las conductas esperadas.

Esto significa que la cultura antisoborno no se construye únicamente mediante documentos.

También se construye mediante:

- Ejemplo de los directivos.
- Comunicación constante.
- Tolerancia cero frente al soborno.
- Reconocimiento de comportamientos íntegros.
- Respuesta adecuada ante incumplimientos.
- Protección de quienes comunican preocupaciones de buena fe.

El ejemplo de la dirección

La conducta de los directivos tiene una influencia directa sobre la cultura de la organización.

Si la dirección exige el cumplimiento de las normas pero permite excepciones cuando se trata de operaciones importantes, clientes estratégicos o personas con posiciones de poder, el mensaje real puede ser contrario a la política antisoborno.

Por ello, **la dirección debe actuar como ejemplo de integridad** y demostrar que las reglas se aplican de manera coherente.

Apoyo a la comunicación de preocupaciones

La alta dirección debe promover el uso de los mecanismos establecidos para comunicar **sospechas o posibles casos de soborno**.

También debe existir un compromiso con la protección de las personas que realizan comunicaciones de buena fe o sobre la base de una creencia razonable, evitando represalias, discriminación o medidas disciplinarias indebidas por haber reportado una preocupación. Esto contribuye a crear un entorno en el que los trabajadores puedan comunicar posibles irregularidades sin temor.

Responsabilidad de la alta dirección

La existencia de una función antisoborno, un responsable de cumplimiento o un área especializada **no elimina la responsabilidad de la alta dirección**. La dirección puede delegar determinadas funciones y responsabilidades, pero debe mantener la supervisión y asegurar que el sistema alcance los resultados previstos. Por ello, el liderazgo debe entenderse como una responsabilidad permanente y no como una actividad realizada únicamente durante la implementación o durante una auditoría.

El papel de la alta dirección en términos prácticos

Para efectos del curso, puede resumirse el papel de la alta dirección en cinco acciones fundamentales:

Establecer: definir la política y los objetivos antisoborno.

Integrar: incorporar los controles antisoborno en los procesos de la organización.

Proporcionar: asegurar los recursos necesarios.

Comunicar: transmitir la importancia de prevenir y combatir el soborno.

Supervisar: revisar que el sistema funcione y contribuya a los resultados previstos.

Estas acciones deben estar acompañadas por un **comportamiento coherente y visible de los líderes**.

Idea clave

La ISO 37001:2025 plantea el liderazgo como un elemento esencial del Sistema de Gestión Antisoborno. **La alta dirección no solo debe aprobar una política: debe demostrar con sus decisiones, recursos, comunicaciones y comportamiento que la organización realmente está comprometida con la prevención del soborno.**

3.2. Función de cumplimiento (oficial de cumplimiento)

Introducción

La **función antisoborno** es un elemento fundamental del Sistema de Gestión Antisoborno establecido por la **ISO 37001:2025**. La norma utiliza el concepto de anti-bribery function para referirse a la persona o conjunto de personas que tienen la **responsabilidad y autoridad para operar el Sistema de Gestión Antisoborno**.

En la práctica, esta función puede estar a cargo de una persona, un equipo o un área especializada, dependiendo del **tamaño, estructura, actividades y nivel de riesgo de la organización**.

Es importante aclarar que la ISO 37001 no establece que todas las organizaciones deban utilizar necesariamente el cargo denominado **"Oficial de Cumplimiento"**. Lo esencial es que exista una **función con responsabilidades y autoridad claramente definidas** para gestionar los aspectos antisoborno.

¿Cuál es el objetivo de la función antisoborno?

La función antisoborno tiene como finalidad ayudar a garantizar que el Sistema de Gestión Antisoborno:

se implemente correctamente, funcione de manera adecuada, se mantenga y se mejore continuamente.

Entre sus principales responsabilidades se encuentran:

- Asegurar que el Sistema de Gestión Antisoborno sea conforme con los requisitos de ISO 37001.
- Supervisar el diseño y la implementación del sistema.
- Informar sobre el desempeño del sistema al órgano de gobierno y a la alta dirección.
- Orientar a la organización respecto de cuestiones relacionadas con el soborno.
- Supervisar determinados procesos y controles antisoborno.
- Promover el conocimiento y cumplimiento de la política antisoborno.

La función antisoborno constituye, por tanto, un **mecanismo especializado de supervisión y apoyo**, pero no sustituye la responsabilidad general de la alta dirección.

Responsabilidad y autoridad

Un aspecto especialmente importante es que la función antisoborno debe contar con **autoridad suficiente para desempeñar sus responsabilidades**.

No tendría sentido designar a una persona como responsable del sistema si no tiene acceso a la información necesaria, capacidad para comunicarse con la dirección o posibilidad de plantear preocupaciones relacionadas con posibles riesgos o incumplimientos.

La organización debe definir claramente:

- Qué responsabilidades tiene la función antisoborno.
- Qué autoridad posee.
- A quién reporta.
- Qué información puede solicitar.
- Cómo comunica sus resultados.
- Cómo participa en la supervisión del sistema.

Independencia y posición dentro de la organización

La función antisoborno debe poder desempeñar sus responsabilidades con un nivel adecuado de **independencia y autoridad**, de acuerdo con la estructura y circunstancias de la organización.

Esto resulta especialmente importante cuando existen situaciones potencialmente sensibles.

Por ejemplo, si una investigación involucra a un proveedor importante o a un directivo, la persona responsable del sistema debe poder **comunicar la situación a los niveles correspondientes sin que las relaciones comerciales o jerárquicas impidan informar adecuadamente**.

La independencia no significa necesariamente que la función deba estar completamente separada de todas las demás áreas. Significa que debe disponer de la **autoridad necesaria para cumplir su función de manera objetiva y efectiva**.

Relación con la alta dirección

La función antisoborno trabaja en estrecha relación con la **alta dirección**, pero sus responsabilidades no deben confundirse. La alta dirección mantiene la **responsabilidad general por la implementación y cumplimiento del Sistema de Gestión Antisoborno**.

La función antisoborno, por su parte, proporciona apoyo especializado, supervisión y seguimiento del sistema.

En términos sencillos:

La alta dirección lidera y responde por el sistema.

La función antisoborno supervisa, asesora e informa sobre su funcionamiento.

Esta separación permite establecer responsabilidades claras y evita que toda la gestión antisoborno dependa exclusivamente de una sola persona.

¿Quién puede ejercer la función antisoborno?

La organización puede determinar la estructura más adecuada según sus características.

En una organización pequeña, la función podría estar asignada a **una sola persona** que tenga otras responsabilidades compatibles. En una organización mediana, podría existir un responsable de compliance o antisoborno con apoyo de otras áreas.

En una organización grande, podría existir un **equipo especializado** con diferentes funciones relacionadas con compliance, riesgos, auditoría o integridad. Lo importante es que la estructura elegida permita cumplir adecuadamente las responsabilidades establecidas por el sistema.

Conocimientos y competencias

Las personas que desempeñan la función antisoborno deben contar con las **competencias necesarias para realizar sus responsabilidades**.

Estas competencias pueden incluir conocimientos sobre:

- Principios de gestión antisoborno.
- Identificación y evaluación de riesgos.
- Controles internos.
- Debida diligencia.
- Legislación y requisitos aplicables.
- Gestión de conflictos de interés.
- Investigación de posibles incidentes.
- Auditoría y seguimiento.
- Comunicación y capacitación.

La formación necesaria dependerá del nivel de responsabilidad y de las características de la organización.

Comunicación de resultados

Una de las funciones esenciales es **informar sobre el desempeño del Sistema de Gestión Antisoborno al órgano de gobierno y a la alta dirección**.

Estos informes pueden abordar, según corresponda:

- Resultados de evaluaciones de riesgos.
- Estado de los controles.
- Incidentes o preocupaciones comunicadas.
- Resultados de auditorías.
- Situaciones de incumplimiento.
- Acciones correctivas.
- Necesidades de recursos.
- Estado de los objetivos antisoborno.
- Oportunidades de mejora.

La comunicación permite que la dirección pueda **tomar decisiones basadas en información relevante sobre el funcionamiento del sistema**.

Asesoramiento a la organización

La función antisoborno también puede desempeñar un papel de **asesoramiento interno**. Por ejemplo, una unidad de compras puede consultar si una determinada relación con un proveedor presenta un riesgo antisoborno.

La función correspondiente puede ayudar a determinar:

- Qué riesgos deben considerarse.
- Si es necesaria una debida diligencia.
- Qué controles pueden aplicarse.
- Si existe un posible conflicto de interés.
- Qué documentación debe conservarse.
- Si la operación requiere una revisión adicional.

De esta manera, la función antisoborno no actúa únicamente cuando ya ocurrió un incidente, sino que también contribuye a la **prevención**.

Función antisoborno y cultura de integridad

La función antisoborno también puede contribuir a desarrollar una **cultura de integridad y cumplimiento** dentro de la organización.

Esto puede realizarse mediante:

- Capacitación.
- Comunicaciones internas.
- Campañas de sensibilización.
- Orientación a los trabajadores.
- Difusión de la política antisoborno.
- Explicación de los canales de denuncia.
- Promoción de comportamientos éticos.

La ISO 37001:2025 pone especial énfasis en la importancia de una **cultura antisoborno y de integridad** dentro de la organización.

La función antisoborno no es un “policía interno”

Es importante evitar una interpretación equivocada de esta función. El responsable antisoborno **no existe únicamente para buscar culpables o sancionar trabajadores**. Su función principal es contribuir a que la organización tenga un sistema capaz de:

prevenir, detectar y responder frente al soborno.

Esto requiere una combinación de prevención, asesoramiento, supervisión, comunicación, seguimiento e investigación cuando corresponda.

Diferencia entre función antisoborno y auditoría interna

La función antisoborno tampoco debe confundirse automáticamente con la **auditoría interna**. La función antisoborno participa en la operación y supervisión del sistema, mientras que la auditoría interna realiza evaluaciones independientes conforme al programa y criterios establecidos.

En una organización pequeña algunas funciones pueden estar concentradas en pocas personas, pero debe prestarse especial atención a los posibles **conflictos de interés y a la objetividad de las evaluaciones**.

Ejemplo práctico

Una empresa constructora recibe una propuesta de un intermediario que ofrece facilitar la obtención de un contrato público. La función antisoborno puede participar en la evaluación de la situación y determinar si existen **señales de riesgo de soborno**.

Puede recomendar:

- Realizar una debida diligencia del intermediario.
- Revisar sus antecedentes y relaciones relevantes.
- Evaluar la justificación comercial de la contratación.
- Aplicar controles adicionales.
- Documentar las decisiones.
- Elevar la situación a la dirección cuando corresponda.

El objetivo no es simplemente rechazar operaciones, sino **asegurar que las decisiones se adopten de manera controlada y coherente con la política antisoborno**.

Idea clave

La **función antisoborno es el componente especializado encargado de apoyar y supervisar el funcionamiento del Sistema de Gestión Antisoborno**.

Debe disponer de **responsabilidades y autoridad claramente definidas**, contar con las competencias necesarias e informar sobre el desempeño del sistema a los niveles correspondientes.

Sin embargo, **la existencia de una función antisoborno no elimina la responsabilidad de la alta dirección**. El liderazgo y la responsabilidad general permanecen en la dirección, mientras que la función antisoborno proporciona el conocimiento, la supervisión y el seguimiento necesarios para que el sistema pueda funcionar eficazmente.

3.3. Elaboración de una política antisoborno

Introducción

La **política antisoborno** es uno de los elementos fundamentales del Sistema de Gestión Antisoborno. La **ISO 37001:2025** establece requisitos específicos para que la alta

dirección establezca una política que defina el compromiso de la organización con la prevención y el rechazo del soborno.

La política no debe entenderse simplemente como un documento administrativo. Su finalidad es establecer una **posición clara de la organización frente al soborno**, orientar el comportamiento de las personas y proporcionar un marco para desarrollar objetivos, controles y demás medidas antisoborno.

En Perú, la norma técnica nacional vigente correspondiente es la **NTP-ISO 37001:2025**, publicada por INACAL en agosto de 2025, que reemplazó a la edición anterior NTP-ISO 37001:2017.

¿Qué es una política antisoborno?

La política antisoborno es una declaración formal mediante la cual la organización establece sus **principios y compromisos fundamentales para prevenir, detectar y responder frente al soborno**.

Debe expresar de manera clara que la organización:

- **Prohíbe el soborno.**
- Se compromete a cumplir las leyes antisoborno aplicables.
- Promueve una cultura de integridad.
- Establece un marco para definir objetivos antisoborno.
- Facilita la comunicación de preocupaciones de buena fe.
- Se compromete con la mejora continua del Sistema de Gestión Antisoborno.
- Reconoce la autoridad e independencia de la función antisoborno.
- Establece las consecuencias de incumplir la política.

Estos elementos forman parte de los requisitos establecidos para la política antisoborno en ISO 37001:2025.

La responsabilidad de la alta dirección

La política antisoborno debe ser **establecida por la alta dirección**. Esto es importante porque la política representa el compromiso oficial de la organización y no simplemente una iniciativa de un departamento determinado.

La alta dirección debe asegurarse de que la política sea coherente con:

- El propósito de la organización.
- Sus actividades.
- Sus riesgos de soborno.
- Sus obligaciones legales.
- Su estructura y contexto.
- Sus objetivos estratégicos.

Por ello, una política antisoborno no debería ser un documento genérico copiado de otra organización. **Debe reflejar las características reales de la organización y los riesgos a los que está expuesta.**

Prohibición del soborno

Uno de los elementos esenciales de la política es establecer claramente que **el soborno está prohibido**. La organización debe adoptar una posición inequívoca frente a cualquier conducta que implique ofrecer, prometer, entregar, solicitar o aceptar una ventaja indebida con la finalidad de influir en una decisión o actuación.

La prohibición debe aplicarse de manera coherente a las actividades de la organización y, según corresponda, a las relaciones con sus trabajadores y socios de negocio. Una política que utiliza expresiones demasiado generales, como simplemente **"actuar éticamente"**, puede resultar insuficiente para comunicar claramente la posición de la organización frente al soborno.

Cumplimiento de las leyes antisoborno

La política debe incluir el compromiso de **cumplir las leyes antisoborno aplicables a la organización**. Esto es especialmente relevante para organizaciones que operan en diferentes países o sectores regulados.

En una organización que desarrolla actividades en Perú, la política debe implementarse teniendo en cuenta el **marco jurídico peruano aplicable**, además de cualquier otra legislación que pueda resultar aplicable por la naturaleza de sus operaciones, relaciones comerciales o presencia internacional. La política no sustituye la legislación.

La política establece el compromiso y las reglas internas de la organización, mientras que la legislación establece las obligaciones jurídicas que deben cumplirse.

Adaptación al contexto de la organización

La política debe ser **apropiada al propósito y contexto de la organización**. Una empresa minera, una empresa constructora, una municipalidad y una empresa de servicios pueden tener riesgos de soborno muy diferentes.

Por ejemplo, una organización que participa frecuentemente en procesos de contratación pública puede enfrentarse a riesgos relacionados con:

- Funcionarios públicos.
- Contrataciones.
- Intermediarios.
- Licencias y autorizaciones.
- Proveedores.
- Contratistas.

En cambio, una empresa dedicada principalmente a operaciones comerciales privadas puede presentar otros escenarios de riesgo. Por ello, **la política debe ser comprensible y relevante para las actividades reales de la organización**.

Marco para establecer objetivos antisoborno

La política también debe proporcionar un **marco para establecer objetivos antisoborno**. Esto significa que la política no debe quedarse únicamente en una declaración de principios. Debe permitir que la organización transforme sus compromisos generales en objetivos concretos.

Por ejemplo, una organización podría establecer objetivos relacionados con:

- Capacitación del personal expuesto a riesgos.
- Evaluación de socios de negocio.
- Fortalecimiento de controles financieros.
- Revisión de determinados procesos.
- Gestión de denuncias.
- Realización de auditorías.
- Reducción de determinadas exposiciones al riesgo.

Los objetivos deben estar relacionados con las necesidades y riesgos reales de la organización.

Compromiso con la mejora continua

La política debe incluir un **compromiso con la mejora continua del Sistema de Gestión Antisoborno**. Esto significa que la organización no debería considerar que la política queda terminada definitivamente después de su aprobación.

El contexto puede cambiar, pueden aparecer nuevos riesgos, pueden modificarse las operaciones y pueden detectarse deficiencias en los controles. Por ello, la política y el sistema deben revisarse cuando sea necesario para garantizar que continúan siendo adecuados.

Promoción de la comunicación de preocupaciones

La política debe fomentar que las personas puedan **plantear preocupaciones de buena fe o sobre la base de una creencia razonable**, de manera confidencial y sin temor a represalias.

Este principio es importante porque un sistema antisoborno necesita mecanismos que permitan detectar situaciones que no necesariamente son visibles mediante controles financieros o auditorías.

Los trabajadores y otras personas relacionadas con la organización deben saber:

- Dónde comunicar una preocupación.
- Cómo realizar una denuncia o reporte.
- Qué tipo de situaciones deben comunicarse.
- Qué protección existe frente a represalias.
- Qué tratamiento recibirá la información.

Autoridad e independencia de la función antisoborno

La política también debe explicar la **autoridad y la independencia de la función antisoborno**. Esto conecta directamente con el punto anterior del curso.

La persona o función responsable del sistema debe tener suficiente autoridad para desempeñar sus responsabilidades y comunicar situaciones relevantes a los niveles correspondientes.

La política puede establecer de manera general este compromiso, mientras que los procedimientos internos pueden definir posteriormente las responsabilidades y mecanismos específicos.

Consecuencias del incumplimiento

Otro elemento importante es establecer que existen **consecuencias frente al incumplimiento de la política antisoborno**. Estas consecuencias deben estar relacionadas con las normas internas de la organización y con la legislación aplicable.

La política puede establecer el principio general de que las infracciones serán tratadas de acuerdo con los procedimientos internos correspondientes. Esto ayuda a evitar la percepción de que la política es únicamente una declaración simbólica.

Una política efectiva debe dejar claro que sus principios tienen consecuencias prácticas.

Comunicación de la política

La política antisoborno debe estar disponible como **información documentada** y debe ser comunicada dentro de la organización. También debe estar disponible para las partes interesadas cuando corresponda y comunicarse a los socios de negocio que presenten un riesgo de soborno superior al bajo.

La comunicación puede realizarse mediante diferentes mecanismos:

- Inducción de nuevos trabajadores.
- Capacitación.
- Intranet.
- Correo institucional.
- Manuales internos.
- Reuniones.
- Página web corporativa.
- Materiales de sensibilización.

El objetivo no es simplemente demostrar que existe un documento, sino conseguir que **las personas conozcan la política y comprendan lo que significa para sus actividades**.

Lenguaje claro y comprensible

Una política antisoborno debe utilizar un lenguaje **claro, directo y comprensible** para las personas a las que está dirigida. No es recomendable elaborar una política excesivamente técnica que solamente pueda entender el departamento legal.

Un trabajador de compras, un supervisor de operaciones o un empleado administrativo debe poder comprender fácilmente:

qué está prohibido, qué se espera de él y qué debe hacer si identifica una situación sospechosa.

Política y realidad organizacional

Uno de los mayores errores en la elaboración de una política antisoborno es crear un documento formal que **no corresponde con las prácticas reales de la organización**.

Por ejemplo, no sería coherente declarar una tolerancia absoluta frente al soborno y, al mismo tiempo, permitir informalmente determinados pagos o beneficios para acelerar trámites. La política debe reflejar el comportamiento que la organización realmente está dispuesta a exigir.

La credibilidad de la política depende de la coherencia entre lo que se declara y lo que se hace.

Política antisoborno y socios de negocio

La política también debe tener relevancia para los **socios de negocio**. En determinadas relaciones, especialmente cuando existe un riesgo de soborno superior al bajo, la organización debe comunicar sus expectativas antisoborno y aplicar los controles correspondientes.

Esto es particularmente importante cuando terceros actúan en nombre de la organización o tienen contacto con clientes, autoridades u otros actores relevantes.

Ejemplo de una política básica

Una organización podría estructurar su declaración de política alrededor de los siguientes compromisos:

La organización prohíbe cualquier forma de soborno, directa o indirecta, relacionada con sus actividades.

La organización se compromete a cumplir las leyes antisoborno aplicables y los requisitos internos establecidos.

La organización promueve una cultura de integridad, transparencia y comportamiento ético.

La organización proporciona canales para comunicar preocupaciones de buena fe, procurando proteger a quienes realizan dichos reportes frente a represalias.

La organización mantiene una función antisoborno con la autoridad e independencia necesarias para desempeñar sus responsabilidades.

La organización establece objetivos antisoborno y revisa periódicamente el desempeño del sistema.

La organización se compromete con la mejora continua de su Sistema de Gestión Antisoborno.

Este contenido constituye una estructura orientativa. La política real debe adaptarse al contexto, tamaño, estructura y riesgos de cada organización.

Aprobación y actualización

Una vez elaborada, la política debe pasar por el proceso interno correspondiente de **revisión y aprobación por la alta dirección**.

También debe mantenerse actualizada cuando existan cambios relevantes en:

- La estructura de la organización.
- Sus actividades.
- Los riesgos de soborno.
- El marco legal.
- Las relaciones con socios de negocio.
- Los procesos internos.
- Los objetivos antisoborno.

La revisión permite asegurar que la política continúe siendo **adecuada, pertinente y coherente con el sistema**.

Diferencia entre política y procedimiento

Es importante distinguir entre una **política antisoborno** y un **procedimiento antisoborno**. La política establece principalmente: **qué principios y compromisos asume la organización.**

Los procedimientos establecen: **cómo se aplican esos principios en situaciones concretas.**

Por ejemplo, la política puede establecer que la organización prohíbe el soborno.

Un procedimiento específico puede explicar cómo se debe actuar cuando un trabajador recibe una oferta indebida de un tercero. De esta manera, **la política establece la dirección y los procedimientos permiten llevarla a la práctica**.

Política antisoborno como base del sistema

La política funciona como uno de los puntos de referencia del Sistema de Gestión Antisoborno.

A partir de ella pueden desarrollarse:

- Objetivos antisoborno.
- Evaluaciones de riesgos.
- Controles.
- Programas de capacitación.
- Procedimientos.
- Mecanismos de denuncia.
- Actividades de seguimiento.
- Auditorías.
- Acciones correctivas.

Por ello, una política bien elaborada ayuda a proporcionar **coherencia al conjunto del sistema**.

Aspectos clave para recordar

La **política antisoborno debe ser establecida por la alta dirección** y debe reflejar el compromiso real de la organización con la prevención del soborno.

De acuerdo con ISO 37001:2025, debe incluir, entre otros aspectos, la **prohibición del soborno, el cumplimiento de las leyes aplicables, un marco para establecer objetivos antisoborno, el compromiso con los requisitos aplicables, la promoción de la comunicación de preocupaciones de buena fe, la mejora continua, la autoridad e independencia de la función antisoborno y las consecuencias del incumplimiento**.

Además, debe mantenerse como **información documentada, comunicarse dentro de la organización y ponerse a disposición de las partes correspondientes**.

En definitiva, **una política antisoborno eficaz no es simplemente un documento que se firma y se archiva**. Es la declaración formal mediante la cual la organización establece su posición frente al soborno y proporciona la base para desarrollar un sistema capaz de **prevenir, detectar y responder ante los riesgos de soborno**

3.4. Roles y responsabilidades

Introducción

La implementación de un Sistema de Gestión Antisoborno requiere que **las responsabilidades estén claramente definidas y comunicadas dentro de la organización**. ISO 37001:2025 establece que la responsabilidad frente al sistema no corresponde exclusivamente a la función antisoborno: **la alta dirección, los responsables de cada nivel y todo el personal tienen responsabilidades relacionadas con la prevención y gestión del soborno**.

Una distribución clara de funciones permite evitar situaciones en las que nadie sabe quién debe tomar una decisión, realizar un control, comunicar una preocupación o actuar frente a un posible incumplimiento.

Responsabilidad general de la alta dirección

La **alta dirección mantiene la responsabilidad general por la implementación y el cumplimiento del Sistema de Gestión Antisoborno**.

Entre sus principales responsabilidades se encuentran:

- Establecer y promover la política antisoborno.
- Asegurar que el sistema esté integrado en los procesos de la organización.
- Proporcionar los recursos necesarios.
- Establecer objetivos antisoborno.
- Promover una cultura de integridad.
- Asegurar que las responsabilidades y autoridades sean asignadas y comunicadas.
- Supervisar el desempeño del sistema.
- Revisar periódicamente su funcionamiento.
- Adoptar las medidas necesarias cuando se identifiquen deficiencias.

Delegar determinadas funciones no elimina la responsabilidad general de la alta dirección.

Responsabilidades de los gerentes y responsables de área

Los **gerentes y responsables de cada nivel** tienen un papel fundamental porque deben asegurar que el Sistema de Gestión Antisoborno se aplique dentro de sus respectivas áreas o funciones.

Esto significa que un responsable de compras, por ejemplo, no puede considerar que el antisoborno es exclusivamente responsabilidad del área de cumplimiento.

Debe asegurarse de que dentro de su área se respeten los controles establecidos para:

- Selección de proveedores.
- Contratación de terceros.
- Aprobación de operaciones.
- Gestión de regalos y hospitalidad.
- Evaluación de riesgos.
- Autorización de pagos.
- Comunicación de posibles irregularidades.

La responsabilidad debe trasladarse, por tanto, **desde el nivel estratégico hasta las actividades operativas**.

Responsabilidad de la función antisoborno

La **función antisoborno** tiene responsabilidades y autoridad específicas dentro del sistema.

Entre sus funciones principales se encuentran:

- Verificar que el Sistema de Gestión Antisoborno sea conforme con los requisitos establecidos.
- Supervisar el diseño y la implementación del sistema.
- Informar sobre su desempeño a la alta dirección y al órgano de gobierno.
- Proporcionar orientación y asesoramiento sobre cuestiones relacionadas con el soborno.
- Apoyar la identificación y gestión de riesgos antisoborno.
- Promover la aplicación de las políticas y controles correspondientes.
- Supervisar determinados aspectos del funcionamiento del sistema.

La función antisoborno debe disponer de **recursos adecuados, competencia, autoridad, posición e independencia suficientes** para desempeñar sus responsabilidades. Además, debe tener acceso directo y oportuno a la alta dirección y al órgano de gobierno cuando sea necesario comunicar una preocupación relacionada con el soborno.

Responsabilidades del órgano de gobierno

Cuando la organización cuenta con un **órgano de gobierno**, como un directorio, consejo u otra estructura equivalente, este también desempeña un papel importante en la supervisión del sistema.

El órgano de gobierno puede participar en:

- Supervisión del compromiso de la alta dirección.
- Revisión de información relevante sobre el sistema.
- Supervisión de los riesgos significativos.
- Seguimiento del desempeño antisoborno.
- Recepción de información sobre situaciones relevantes.
- Supervisión de la eficacia del sistema.

En organizaciones pequeñas puede ocurrir que **no exista una separación clara entre órgano de gobierno y alta dirección**. En esos casos, las mismas personas pueden ejercer ambas funciones, dependiendo de la estructura de la organización.

Responsabilidades de todo el personal

El Sistema de Gestión Antisoborno no funciona únicamente mediante los directivos y especialistas de cumplimiento.

Todo el personal tiene responsabilidades relacionadas con el sistema en función de su puesto y actividades.

Entre ellas se encuentran:

- Conocer la política antisoborno.
- Cumplir los procedimientos y controles aplicables.
- Participar en las capacitaciones correspondientes.
- Actuar de acuerdo con las normas internas.

- Evitar conductas que puedan constituir soborno.
- Comunicar posibles incumplimientos o situaciones sospechosas.
- Cooperar con las investigaciones cuando corresponda.
- Informar sobre conflictos o situaciones que puedan generar riesgos.

ISO señala expresamente que todos los trabajadores tienen responsabilidades relacionadas con conocer y cumplir la política antisoborno, completar la capacitación correspondiente y comunicar posibles casos de incumplimiento.

Responsabilidades según el puesto

No todos los trabajadores tienen las mismas responsabilidades.

La organización debe establecer las funciones de acuerdo con **la posición, autoridad, actividades y exposición al riesgo de cada persona**.

Por ejemplo, un trabajador administrativo puede tener responsabilidades básicas de cumplimiento de la política y comunicación de irregularidades.

Un trabajador de compras puede tener responsabilidades adicionales relacionadas con:

- Evaluación de proveedores.
- Debida diligencia.
- Conflictos de interés.
- Regalos y hospitalidad.
- Procesos de contratación.

Un gerente puede tener responsabilidades relacionadas con:

- Aprobación de operaciones.
- Supervisión de controles.
- Gestión de riesgos.
- Asignación de recursos.
- Seguimiento del cumplimiento.

De esta manera, **las responsabilidades deben ser proporcionales al nivel de autoridad y exposición al riesgo**.

Delegación de responsabilidades

En organizaciones complejas, determinadas decisiones pueden ser delegadas a otras personas.

Sin embargo, cuando se delegan decisiones relacionadas con situaciones que presentan **más que un riesgo bajo de soborno**, la organización debe establecer procesos o controles que permitan asegurar que:

- La persona tenga autoridad suficiente.
- La decisión se adopte mediante un proceso definido.
- Se consideren los riesgos de soborno.

- Se eviten conflictos de interés reales o potenciales.
- Exista una supervisión adecuada.

La delegación de una decisión **no significa que la alta dirección deje de tener sus responsabilidades frente al sistema**.

Conflictos de interés

La distribución de responsabilidades debe considerar también los **conflictos de interés**.

Una persona que participa en una decisión de alto riesgo no debería encontrarse en una situación en la que sus intereses personales, familiares, económicos o profesionales puedan afectar su objetividad.

Por ello, la organización debe establecer mecanismos adecuados para:

- Identificar conflictos de interés.
- Declararlos.
- Evaluarlos.
- Gestionarlos.
- Documentar las medidas adoptadas.

Esto resulta especialmente importante en áreas como **compras, contrataciones, selección de proveedores, proyectos y relaciones con terceros**.

Responsabilidades en las decisiones de alto riesgo

Cuando una decisión puede presentar un riesgo significativo de soborno, la organización puede establecer **niveles adicionales de revisión y autorización**. Por ejemplo, una contratación de un intermediario que tendrá contacto con funcionarios públicos podría requerir:

evaluación del riesgo → debida diligencia → revisión de cumplimiento → aprobación por el nivel correspondiente → documentación de la decisión.

El objetivo es evitar que una sola persona pueda tomar decisiones sensibles sin controles adecuados.

Responsabilidades de los socios de negocio

El sistema también debe considerar a los **socios de negocio**, especialmente cuando actúan en nombre de la organización o pueden generar una exposición significativa al riesgo de soborno.

Dependiendo del nivel de riesgo, la organización puede establecer requisitos relacionados con:

- Debida diligencia.

- Compromisos antisoborno.
- Cláusulas contractuales.
- Capacitación o comunicación.
- Supervisión.
- Controles sobre pagos.
- Seguimiento del comportamiento del tercero.

ISO 37001 contempla controles y medidas relacionadas con los socios de negocio, incluidos procesos de debida diligencia y medidas proporcionales al riesgo.

Comunicación de las responsabilidades

No basta con definir responsabilidades en un documento interno. **Las responsabilidades deben ser comunicadas a las personas correspondientes**, de manera que cada trabajador comprenda qué se espera de él.

Esto puede realizarse mediante:

- Manuales internos.
- Descripciones de puestos.
- Políticas.
- Procedimientos.
- Capacitaciones.
- Reuniones.
- Comunicaciones internas.
- Programas de inducción.

La comunicación debe ser especialmente clara cuando una persona tiene **autoridad para aprobar operaciones, contratar terceros o tomar decisiones relacionadas con riesgos de soborno**.

Ejemplo práctico

Una empresa constructora participa en una licitación pública. En este proceso pueden intervenir diferentes personas y áreas:

Alta dirección: establece las políticas y proporciona los recursos necesarios.

Gerencia del proyecto: supervisa que las actividades se desarrollen conforme a las reglas establecidas.

Área de compras: aplica los controles correspondientes a proveedores y terceros.

Función antisoborno: asesora, supervisa y comunica los riesgos o situaciones relevantes.

Área financiera: aplica los controles establecidos para pagos y transacciones.

Trabajadores: cumplen las políticas y comunican cualquier situación sospechosa.

Socios de negocio: deben cumplir los requisitos antisoborno establecidos en sus relaciones con la organización.

Este ejemplo demuestra que **el sistema funciona como una estructura de responsabilidades conectadas**, y no como una tarea aislada del responsable de cumplimiento.

Matriz de responsabilidades

Una herramienta práctica para organizar estas funciones es la **matriz de responsabilidades**. La organización puede establecer una tabla en la que se indique quién es responsable de cada actividad.

Por ejemplo:

Actividad	Responsable principal	Supervisión
Política antisoborno	Alta dirección	Órgano de gobierno
Evaluación de riesgos	Función antisoborno / responsables de área	Alta dirección
Debida diligencia	Área responsable / función antisoborno	Dirección
Capacitación	Recursos Humanos / función antisoborno	Alta dirección
Controles financieros	Área financiera	Dirección
Denuncias	Función antisoborno	Alta dirección / órgano de gobierno
Auditoría interna	Auditoría interna	Dirección / órgano correspondiente
Acciones correctivas	Responsable del proceso	Función antisoborno

La estructura concreta dependerá del **tamaño, complejidad y organización interna de cada entidad**.

Responsabilidad compartida

Una de las ideas más importantes de este apartado es que **la prevención del soborno es una responsabilidad compartida**.

La alta dirección establece el liderazgo y mantiene la responsabilidad general. Los gerentes aseguran la aplicación del sistema dentro de sus áreas. La función antisoborno proporciona supervisión, asesoramiento e información especializada. Los trabajadores cumplen las reglas y comunican posibles irregularidades. Los socios de negocio deben respetar los requisitos que les sean aplicables.

Por tanto, **un sistema antisoborno eficaz requiere que cada persona conozca su papel y actúe de acuerdo con él**.

Idea clave

ISO 37001:2025 establece una estructura clara de **roles, responsabilidades y autoridades**.

La **alta dirección tiene la responsabilidad general** del Sistema de Gestión Antisoborno, mientras que los gerentes deben asegurar su aplicación dentro de sus áreas. La **función antisoborno** desempeña una función especializada de supervisión, asesoramiento e información, con la autoridad e independencia necesarias. Finalmente, **todo el personal debe conocer, cumplir y aplicar las medidas antisoborno que correspondan a su función**.

El objetivo final es que la responsabilidad frente al soborno **no dependa de una sola persona**, sino que forme parte de la estructura normal de gobierno y gestión de la organización.

4. Evaluación de Riesgos y Debida Diligencia

4.1. Metodología de evaluación de riesgos

Introducción

La **evaluación del riesgo de soborno** constituye uno de los elementos centrales de un Sistema de Gestión Antisoborno conforme a **ISO 37001:2025**. La norma establece específicamente que la organización debe realizar evaluaciones del riesgo de soborno a intervalos planificados, identificar los riesgos que puede anticipar razonablemente, analizarlos, evaluarlos, priorizarlos y comprobar si los controles existentes son adecuados y eficaces.

La finalidad no es conseguir que el riesgo de soborno desaparezca completamente, algo que ninguna metodología puede garantizar. El objetivo es **conocer dónde, cómo y por qué puede producirse el soborno**, determinar qué riesgos son prioritarios y establecer medidas proporcionales para prevenirlo, detectarlo y responder ante él.

Por esta razón, la evaluación de riesgos debe servir como una **base práctica para tomar decisiones**, asignar recursos y determinar qué controles antisoborno necesita realmente la organización.

¿Qué es el riesgo de soborno?

El **riesgo de soborno** es la posibilidad de que se produzca una conducta relacionada con el soborno que pueda afectar a la organización, sus actividades, sus trabajadores o sus relaciones con terceros.

Este riesgo puede aparecer tanto dentro de la organización como a través de **personas o entidades que actúan en su nombre o mantienen relaciones comerciales con ella**.

Por ejemplo, puede existir riesgo cuando una organización:

- Contrata proveedores o intermediarios.
- Participa en licitaciones.
- Solicita permisos o autorizaciones.
- Mantiene relaciones con funcionarios públicos.
- Realiza operaciones comerciales de alto valor.
- Trabaja en sectores con elevada exposición regulatoria.
- Opera en diferentes países.
- Entrega o recibe regalos y hospitalidad.
- Realiza donaciones o patrocinios.
- Gestiona proyectos complejos.
- Utiliza agentes, representantes o consultores.

El riesgo debe analizarse en función de las actividades reales de la organización y de su contexto, no únicamente mediante una lista genérica de riesgos.

Objetivo de la metodología

La metodología de evaluación debe permitir responder, como mínimo, a cuatro preguntas fundamentales:

¿Qué puede ocurrir?

Identificar los posibles escenarios de soborno.

¿Qué tan importante es el riesgo?

Analizar la probabilidad y las posibles consecuencias.

¿Qué riesgos deben atenderse primero?

Priorizar los riesgos según criterios previamente establecidos.

¿Los controles existentes funcionan?

Determinar si las medidas actuales son adecuadas y eficaces para reducir el riesgo. Estos elementos corresponden directamente al enfoque establecido en el apartado **4.5 de ISO 37001:2025**.

Establecimiento de criterios de evaluación

Antes de evaluar los riesgos, la organización debe establecer **criterios para determinar el nivel de riesgo de soborno**. ISO 37001:2025 establece que estos criterios deben considerar las **políticas y objetivos de la organización**.

Una organización puede establecer, por ejemplo, tres niveles:

Riesgo bajo: exposición limitada y controles suficientes.

Riesgo medio: exposición significativa que requiere controles adicionales o seguimiento.

Riesgo alto: exposición importante que requiere medidas reforzadas, supervisión y atención prioritaria.

También pueden utilizarse cinco niveles, como muy bajo, bajo, medio, alto y muy alto. Lo importante es que los criterios sean **claros, coherentes y aplicables de manera consistente**.

Identificación de los riesgos

El primer paso práctico consiste en identificar los posibles escenarios en los que podría producirse un soborno. No se trata simplemente de escribir “riesgo de soborno” en una matriz. Es necesario describir **cómo podría producirse el hecho**.

Por ejemplo:

“Un intermediario ofrece un pago indebido a un funcionario público para acelerar la obtención de una autorización necesaria para el proyecto.”

Este planteamiento es mucho más útil que una descripción genérica porque permite posteriormente identificar:

- Quién podría intervenir.
- En qué proceso podría ocurrir.
- Qué beneficio se pretende obtener.
- Qué controles deberían existir.
- Cómo podría detectarse.

Identificación de factores de riesgo

Para identificar adecuadamente los riesgos, deben considerarse los factores relacionados con el **contexto de la organización**, sus actividades y las relaciones que mantiene.

Entre los aspectos que pueden analizarse se encuentran:

- Naturaleza de las actividades.
- Tamaño y estructura de la organización.
- Ubicación geográfica.
- Sectores en los que opera.
- Tipo de clientes.
- Relaciones con entidades públicas.
- Uso de intermediarios.
- Proveedores y contratistas.
- Socios de negocio.
- Procesos de contratación.
- Operaciones financieras.
- Regalos y hospitalidad.
- Donaciones y patrocinios.
- Licencias, permisos y autorizaciones.
- Proyectos de alto valor.
- Cambios recientes en la organización.

La evaluación debe centrarse en los factores que realmente pueden generar exposición al soborno.

Análisis del riesgo

Una vez identificados los riesgos, deben ser **analizados**. El análisis busca determinar las características del riesgo y su nivel de exposición. Una metodología práctica puede considerar dos dimensiones principales:

Probabilidad: posibilidad de que el escenario de soborno ocurra.

Impacto: consecuencias que podría generar si ocurre.

Por ejemplo, una organización puede utilizar una escala de 1 a 5 para cada dimensión.

Probabilidad	Descripción
1	Muy baja
2	Baja
3	Media
4	Alta
5	Muy alta

Y una escala similar para el impacto. La combinación de ambas variables permite obtener una valoración inicial del riesgo.

Riesgo inherente y riesgo residual

Una metodología más desarrollada puede diferenciar entre **riesgo inherente** y **riesgo residual**. El **riesgo inherente** representa la exposición existente antes de considerar los controles implementados.

Por ejemplo, una empresa que realiza frecuentemente trámites ante autoridades públicas puede presentar una exposición inherente considerable, especialmente si depende de múltiples permisos y autorizaciones. El **riesgo residual** representa el nivel de riesgo que permanece después de considerar los controles existentes.

Esta diferencia es importante porque permite evaluar si los controles realmente están reduciendo la exposición.

Evaluación de los controles existentes

ISO 37001:2025 no exige únicamente identificar y valorar riesgos. También exige **evaluar la idoneidad y eficacia de los controles existentes para mitigar los riesgos identificados**. Por ello, después de identificar un riesgo es necesario preguntarse:

¿Qué controles existen actualmente?

Por ejemplo:

- Separación de funciones.
- Aprobaciones.
- Límites de autorización.
- Debida diligencia.
- Controles financieros.
- Supervisión.
- Capacitación.
- Declaraciones de conflictos de interés.
- Canal de denuncias.
- Auditorías.
- Cláusulas contractuales.

Pero no basta con comprobar que el control existe. También debe analizarse **si realmente funciona**.

Adecuación y eficacia de los controles

Un control puede existir formalmente y, sin embargo, ser insuficiente.

Por ejemplo, una empresa puede tener una política que exige autorización para determinados pagos, pero si en la práctica los pagos se realizan sin la autorización requerida, el control **no está funcionando eficazmente**.

Por eso deben analizarse aspectos como:

- Si el control está correctamente diseñado.
- Si se aplica realmente.
- Si se aplica de manera consistente.
- Si existe evidencia de su aplicación.
- Si permite reducir el riesgo.
- Si necesita ser reforzado.

La existencia de un procedimiento no demuestra por sí sola que el riesgo esté controlado.

Priorización de los riesgos

Después del análisis, los riesgos deben ser **priorizados**. No todos los riesgos requieren exactamente el mismo nivel de atención.

La organización debe concentrar mayores recursos en los escenarios que puedan generar una exposición significativa.

Por ejemplo:

Riesgo bajo: puede mantenerse mediante controles básicos y seguimiento.

Riesgo medio: puede requerir controles adicionales y supervisión periódica.

Riesgo alto: puede requerir medidas reforzadas, aprobación de niveles superiores, debida diligencia más profunda y seguimiento específico.

Este enfoque permite aplicar un principio fundamental de ISO 37001: **las medidas antisoborno deben ser razonables y proporcionales al nivel de riesgo**.

Matriz de riesgo de soborno

Una herramienta práctica para organizar la evaluación es la **matriz de riesgos**.

Por ejemplo:

Riesgo	Probabilidad	Impacto	Nivel	Control existente
Pago indebido a funcionario	4	5	Alto	Aprobación y supervisión
Soborno mediante intermediario	4	5	Alto	Debida diligencia
Regalo inapropiado a cliente	3	3	Medio	Política de regalos
Pago irregular a proveedor	2	4	Medio	Separación de funciones

La organización puede utilizar diferentes sistemas de puntuación. **ISO 37001 no impone una única fórmula matemática para calcular el riesgo**; la metodología y los criterios deben ser definidos por la propia organización de acuerdo con su contexto.

Ejemplo aplicado a una empresa minera

Una empresa minera necesita obtener determinadas autorizaciones para desarrollar un proyecto. Durante la evaluación identifica el siguiente escenario:

“Un intermediario podría ofrecer dinero o una ventaja indebida a un funcionario para acelerar la obtención de una autorización.”

La organización puede analizar:

Probabilidad: alta, debido al número y complejidad de las autorizaciones.

Impacto: alto, porque el proyecto podría verse afectado legal, financiera y reputacionalmente.

Riesgo: alto.

Después se revisan los controles existentes:

- Debida diligencia del intermediario.
- Contrato con cláusulas antisoborno.
- Aprobación previa de pagos.
- Prohibición de pagos en efectivo no autorizados.
- Supervisión de la relación.
- Canal de denuncias.

Si los controles se consideran insuficientes, la organización debe establecer **acciones adicionales para reducir el riesgo**.

Ejemplo aplicado a contrataciones con el Estado

Una empresa que participa en contrataciones públicas puede identificar diferentes escenarios de riesgo:

- Entrega de una ventaja indebida a un funcionario.
- Uso de un intermediario para influir en una decisión.
- Alteración de información.
- Pagos irregulares relacionados con contratos.
- Regalos u hospitalidad destinados a influir en una decisión.
- Conflictos de interés no declarados.

Cada escenario debe ser **evaluado individualmente**, teniendo en cuenta las circunstancias concretas de la organización. Esto permite evitar un error frecuente: considerar que todas las contrataciones públicas presentan exactamente el mismo nivel de riesgo.

Frecuencia de la evaluación

La evaluación del riesgo de soborno debe realizarse **a intervalos planificados**. La organización debe definir la frecuencia apropiada teniendo en cuenta su contexto y nivel de exposición.

Además, ISO 37001:2025 establece que la evaluación debe revisarse cuando exista un **cambio significativo en la estructura o actividades de la organización**.

Por ejemplo, puede ser necesario revisar la evaluación cuando:

- Se ingresa a un nuevo mercado.
- Se adquiere otra empresa.
- Se crea una nueva unidad de negocio.
- Se inicia un proyecto importante.
- Se comienza a trabajar con nuevos tipos de intermediarios.
- Cambia significativamente la estructura organizacional.
- Se modifican las actividades.
- Aparece nueva información relevante.
- Se identifica un nuevo escenario de soborno.

La evaluación como proceso dinámico

El riesgo de soborno **no es estático**. Una organización que hoy presenta un determinado nivel de exposición puede enfrentar una situación completamente diferente después de comenzar operaciones en otro país, contratar nuevos intermediarios o participar en proyectos de mayor valor.

Por eso, la evaluación no debe convertirse en un documento que se realiza una sola vez y después se archiva.

Debe mantenerse actualizada y utilizarse para mejorar continuamente el Sistema de Gestión Antisoborno.

Información documentada

La organización debe conservar **información documentada que demuestre que la evaluación del riesgo de soborno se realizó y que fue utilizada para diseñar o mejorar el Sistema de Gestión Antisoborno**.

La documentación puede incluir:

- Metodología utilizada.
- Criterios de evaluación.
- Matrices de riesgos.
- Identificación de escenarios.
- Resultados de la evaluación.
- Controles existentes.
- Valoración de los controles.
- Priorización.
- Acciones propuestas.
- Responsables.
- Fechas de revisión.

La documentación permite demostrar que la evaluación fue realizada de manera **sistemática y trazable**.

Errores frecuentes en la evaluación de riesgos

Entre los errores más comunes se encuentran:

Realizar una evaluación genérica: utilizar una matriz estándar que no refleja las actividades reales de la organización.

Identificar únicamente riesgos internos: ignorar los riesgos relacionados con terceros e intermediarios.

Confundir existencia con eficacia: considerar que un control funciona simplemente porque existe un procedimiento escrito.

No establecer criterios claros: asignar niveles de riesgo sin explicar cómo se determinaron.

No priorizar: tratar todos los riesgos como si tuvieran la misma importancia.

No actualizar la evaluación: mantener durante años una matriz que ya no refleja la realidad de la organización.

No utilizar los resultados: realizar la evaluación únicamente para cumplir con un requisito documental.

Utilización de los resultados

El resultado de la evaluación debe utilizarse para **tomar decisiones dentro del Sistema de Gestión Antisoborno**.

Los resultados pueden influir en:

- Selección de controles.
- Nivel de debida diligencia.
- Capacitación.
- Recursos destinados a compliance.
- Controles financieros.
- Controles sobre terceros.
- Auditorías.
- Supervisión.
- Objetivos antisoborno.
- Procesos de aprobación.
- Planes de mejora.

Por ello, la evaluación de riesgos constituye una especie de **punto de conexión entre los riesgos identificados y las medidas que la organización decide implementar**.

Relación con la debida diligencia

La evaluación del riesgo también sirve para determinar **cuándo y con qué intensidad debe realizarse la debida diligencia** sobre socios de negocio, proveedores, intermediarios y otras partes relacionadas. Un tercero que presenta un riesgo bajo puede estar sujeto a controles básicos.

Un tercero que presenta un riesgo elevado puede requerir una evaluación mucho más profunda antes de iniciar o continuar la relación.

Este enfoque será desarrollado con mayor detalle en el siguiente apartado del curso: **4.2. Debida diligencia de socios y proveedores**.

Metodología resumida

Una metodología práctica de evaluación puede organizarse en las siguientes etapas:

1. Comprender el contexto: analizar las actividades, estructura, operaciones y relaciones de la organización.

2. Identificar escenarios de soborno: determinar dónde y cómo podría producirse un soborno.

3. Analizar los riesgos: valorar la probabilidad y las posibles consecuencias.

4. Evaluar y priorizar: determinar el nivel de riesgo utilizando criterios previamente definidos.

5. Evaluar los controles: comprobar si las medidas existentes son adecuadas y eficaces.

6. Determinar acciones: establecer medidas adicionales cuando sean necesarias.

7. Documentar: conservar evidencia de la evaluación y de las decisiones adoptadas.

8. Revisar: actualizar la evaluación a intervalos planificados y ante cambios significativos.

Este proceso es coherente con los requisitos establecidos por **ISO 37001:2025, apartado 4.5**, y permite que el Sistema de Gestión Antisoborno se base en los riesgos reales de la organización.

Idea clave

La **evaluación del riesgo de soborno es la base para determinar dónde debe concentrar sus esfuerzos una organización**.

ISO 37001:2025 exige que la organización **identifique, analice, evalúe y priorice los riesgos de soborno**, además de evaluar la idoneidad y eficacia de los controles existentes. También exige establecer criterios para determinar los niveles de riesgo, revisar la evaluación a intervalos planificados y actualizarla cuando existan cambios significativos en la estructura o actividades de la organización.

Una buena metodología no consiste simplemente en llenar una matriz. Su verdadero propósito es **convertir la información sobre los riesgos en decisiones concretas**, permitiendo asignar recursos, fortalecer controles y orientar las actividades de prevención, detección y respuesta frente al soborno.

La evaluación debe ser proporcional, documentada, actualizada y útil para la gestión real de la organización.

4.2. Debida diligencia de socios y proveedores

Introducción

La **debida diligencia** es un proceso fundamental dentro de un Sistema de Gestión Antisoborno porque permite a la organización conocer mejor a las personas y entidades con las que mantiene o pretende establecer relaciones.

En **ISO 37001:2025**, la debida diligencia está directamente relacionada con la evaluación del riesgo de soborno. La norma establece que, cuando se identifica un riesgo **superior al bajo**, la organización debe evaluar con mayor profundidad la naturaleza y el alcance de dicho riesgo respecto de determinadas transacciones, proyectos, actividades, socios de negocio y determinadas posiciones del personal.

La finalidad no es investigar exhaustivamente a todos los proveedores y socios por igual. El principio fundamental es aplicar una **debida diligencia proporcional al nivel de riesgo**.

¿Qué es la debida diligencia?

La debida diligencia es un **proceso destinado a obtener y analizar información suficiente para comprender la naturaleza y el alcance del riesgo de soborno** relacionado con una determinada persona, organización, transacción, proyecto o relación.

En el contexto de ISO 37001:2025, la definición de **business associate o socio de negocio** es amplia. Puede incluir, entre otros:

- Clientes.
- Proveedores.
- Contratistas.
- Subcontratistas.
- Consultores.
- Agentes.
- Intermediarios.
- Distribuidores.
- Representantes.
- Asesores.
- Socios de empresas conjuntas.
- Socios de consorcios.
- Proveedores de servicios externalizados.
- Inversores.

La norma señala que los diferentes tipos de socios de negocio pueden presentar **diferentes tipos y niveles de riesgo de soborno**, por lo que no deben ser tratados necesariamente de la misma manera.

Debida diligencia no significa investigar a todo el mundo de la misma manera

Uno de los principios más importantes es la **proporcionalidad**.

No tendría sentido aplicar el mismo procedimiento a una empresa que suministra material de oficina por un importe reducido y a un intermediario que representa a la organización ante funcionarios públicos en un proyecto de gran valor.

La intensidad de la debida diligencia debe considerar factores como:

- Nivel de riesgo de soborno.
- Naturaleza de la relación.

- Valor de las operaciones.
- Actividades que realizará el tercero.
- Contacto con funcionarios públicos.
- Ubicación geográfica.
- Sector de actividad.
- Estructura de propiedad.
- Uso de intermediarios.
- Historial de cumplimiento.
- Naturaleza del proyecto.
- Duración de la relación.

A mayor exposición al riesgo, mayor debe ser la profundidad de la debida diligencia.

¿Cuándo debe realizarse?

La evaluación de riesgos de soborno debe determinar qué categorías de relaciones requieren una debida diligencia específica. ISO 37001:2025 contempla su aplicación cuando se ha identificado un riesgo de soborno **más que bajo** relacionado con determinadas categorías de:

- Transacciones.
- Proyectos.
- Actividades.
- Socios de negocio.
- Posiciones específicas del personal.

La debida diligencia debe permitir obtener información suficiente para evaluar ese riesgo y debe **actualizarse con una frecuencia definida**, de manera que los cambios y la nueva información puedan ser considerados. Por tanto, la debida diligencia no debe entenderse necesariamente como un procedimiento que se realiza una sola vez al inicio de una relación.

¿Qué información puede analizarse?

Dependiendo del nivel de riesgo, la organización puede recopilar y analizar información relacionada con el tercero.

Por ejemplo:

- Identidad y existencia legal.
- Actividad empresarial.
- Propietarios y beneficiarios finales.
- Estructura societaria.
- Representantes legales.
- Experiencia y trayectoria.
- Relaciones comerciales relevantes.
- Países donde opera.
- Antecedentes de corrupción o soborno.
- Sanciones relevantes.
- Conflictos de interés.
- Relaciones con funcionarios públicos.

- Reputación empresarial.
- Capacidad para prestar los servicios contratados.
- Historial de cumplimiento.
- Existencia de políticas y controles antisoborno.

La información concreta debe determinarse **en función del riesgo y de la naturaleza de la relación**.

Identificación de la propiedad y control

En determinadas relaciones puede ser importante conocer **quién es realmente propietario o quién controla al socio de negocio**. Esto resulta especialmente relevante cuando existen estructuras societarias complejas, diferentes niveles de propiedad o intermediarios.

La organización puede necesitar comprender:

- Quién posee la empresa.
- Quién ejerce el control.
- Quién toma las decisiones.
- Quién representa legalmente a la empresa.
- Quién recibirá los pagos.
- Qué otras entidades están relacionadas.

El objetivo es reducir el riesgo de mantener una relación con una entidad cuya estructura real no sea suficientemente conocida.

Relaciones con funcionarios públicos

Un factor especialmente relevante es determinar si el socio de negocio **mantiene contacto con funcionarios públicos en nombre de la organización**.

Por ejemplo, puede existir una exposición mayor cuando un agente o consultor se encarga de:

- Obtener permisos.
- Gestionar autorizaciones.
- Representar a la empresa ante autoridades.
- Participar en procedimientos administrativos.
- Gestionar licencias.
- Intervenir en contrataciones públicas.
- Facilitar relaciones con organismos estatales.

En estos casos, la organización debe prestar especial atención al riesgo de **soborno indirecto a través de terceros**. ISO 37001 aborda expresamente el soborno directo e indirecto, incluido aquel que puede producirse mediante socios de negocio.

Evaluación de la reputación

La reputación del tercero también puede ser relevante. Una organización puede analizar información disponible sobre posibles:

- Investigaciones.
- Sanciones.
- Casos de corrupción.
- Conductas empresariales cuestionables.
- Conflictos de interés.
- Incumplimientos relevantes.
- Noticias negativas relacionadas con integridad.

Sin embargo, la existencia de una noticia negativa **no significa automáticamente que el tercero deba ser rechazado**. La información debe ser evaluada y relacionada con el nivel de riesgo real.

Capacidad y legitimidad del proveedor

La debida diligencia no debe concentrarse exclusivamente en cuestiones relacionadas con corrupción. También puede ser necesario comprobar si el tercero **realmente tiene capacidad para proporcionar los bienes o servicios contratados**.

Por ejemplo, si una empresa pretende contratar a un consultor por una suma considerable, puede resultar razonable verificar:

- Experiencia profesional.
- Personal disponible.
- Capacidad técnica.
- Historial de proyectos.
- Recursos necesarios.
- Existencia legal.
- Justificación económica de sus honorarios.

Esto ayuda a detectar situaciones en las que un tercero podría estar siendo utilizado simplemente como **vehículo para canalizar pagos indebidos**.

Evaluación de los proveedores

En el caso de los proveedores, la organización puede establecer diferentes niveles de revisión. Un proveedor de bajo riesgo podría estar sujeto a controles básicos relacionados con:

- Identificación.
- Existencia legal.
- Información comercial.
- Condiciones contractuales.

Un proveedor de mayor riesgo podría requerir adicionalmente:

- Información sobre propietarios.
- Evaluación de antecedentes.
- Revisión de conflictos de interés.
- Compromiso antisoborno.
- Revisión de determinadas operaciones.
- Controles sobre pagos.
- Seguimiento periódico.

La categoría de proveedor no determina por sí sola el nivel de riesgo. Lo importante es analizar las características concretas de la relación.

Evaluación de intermediarios

Los **intermediarios** pueden representar una exposición particularmente importante porque pueden actuar en nombre de la organización frente a terceros.

Por ejemplo:

Empresa → intermediario → funcionario público

Si el intermediario ofrece un pago indebido para conseguir una ventaja para la empresa, la organización puede quedar expuesta a consecuencias legales, financieras y reputacionales.

Por ello, antes de contratar a determinados intermediarios puede ser necesario realizar una evaluación más profunda de:

- Su experiencia.
- Sus relaciones.
- Su reputación.
- Sus propietarios.
- Sus vínculos con funcionarios.
- La justificación de su contratación.
- Los servicios que realmente prestará.
- La razonabilidad de sus honorarios.

Justificación de la relación

La organización debe poder explicar **por qué necesita contratar al tercero y qué función realizará**.

Una situación en la que un intermediario recibe una remuneración elevada sin que exista una justificación clara puede constituir una señal de alerta.

Por ello, es recomendable documentar:

- Motivo de la contratación.
- Servicios esperados.
- Alcance de sus funciones.
- Forma de remuneración.

- Responsabilidades.
- Duración de la relación.
- Justificación del precio.

Señales de alerta

Durante la debida diligencia pueden aparecer **señales de alerta** que requieran una investigación adicional.

Algunos ejemplos son:

- El tercero se niega a proporcionar información básica.
- No existe claridad sobre sus propietarios.
- Solicita pagos a cuentas de terceros.
- Solicita pagos en efectivo sin justificación.
- Sus honorarios son desproporcionados.
- Tiene vínculos no declarados con funcionarios públicos.
- No puede demostrar experiencia suficiente.
- Insiste en evitar controles internos.
- Se niega a aceptar cláusulas antisoborno.
- Existen antecedentes relevantes de corrupción.
- La estructura societaria resulta innecesariamente compleja.
- Solicita que determinados pagos sean registrados de forma incorrecta.

Una señal de alerta **no demuestra por sí misma que haya ocurrido un soborno**, pero puede justificar una revisión adicional.

Evaluación de los resultados

Una vez recopilada la información, la organización debe analizar los resultados y determinar qué hacer con ellos.

Puede concluir que:

El riesgo es bajo: la relación puede continuar con controles básicos.

El riesgo es moderado: pueden ser necesarios controles adicionales.

El riesgo es alto: puede requerirse una debida diligencia reforzada y medidas específicas antes de iniciar o continuar la relación.

Existe una situación inaceptable: la organización puede decidir no establecer la relación o tomar medidas para terminarla, de acuerdo con sus procedimientos y obligaciones aplicables.

La decisión debe estar **basada en información y criterios previamente establecidos**, no únicamente en una apreciación subjetiva.

Debida diligencia antes de contratar

Cuando el riesgo lo justifique, la debida diligencia debe realizarse **antes de establecer la relación**.

Por ejemplo, antes de contratar a un agente para representar a una empresa minera ante autoridades públicas, la organización puede:

Identificar al agente → evaluar el riesgo → realizar la debida diligencia → analizar los resultados → aprobar o rechazar la relación → establecer controles contractuales.

Este proceso permite evitar que la organización establezca primero la relación y recién después descubra riesgos importantes.

Debida diligencia durante la relación

La debida diligencia no necesariamente termina con la firma del contrato. La organización debe establecer una **frecuencia definida para actualizarla**, especialmente cuando la relación presenta un riesgo significativo.

Puede ser necesario realizar una nueva revisión cuando:

- Cambia la propiedad del proveedor.
- Cambian los responsables.
- Se amplía el alcance del contrato.
- Aumenta significativamente el valor de las operaciones.
- El tercero comienza a tratar con funcionarios públicos.
- Aparece nueva información relevante.
- Se producen incidentes.
- Cambian las condiciones del proyecto.
- Se detectan nuevas señales de alerta.

Compromisos antisoborno de los socios de negocio

ISO 37001:2025 contempla requisitos específicos para los **compromisos antisoborno de los socios de negocio**.

Cuando un socio presenta un riesgo superior al bajo, la organización debe implementar procedimientos que, en la medida de lo posible, aseguren que el socio se comprometa a **prevenir el soborno relacionado con la relación, transacción, proyecto o actividad correspondiente**.

También debe existir, cuando sea posible, la capacidad de **terminar la relación** en caso de que el socio participe en un soborno relacionado con dicha relación.

Cláusulas contractuales

Una herramienta práctica para gestionar el riesgo es incluir **cláusulas antisoborno en los contratos**.

Estas pueden establecer compromisos relacionados con:

- Prohibición del soborno.
- Cumplimiento de la política antisoborno.
- Cumplimiento de las leyes aplicables.
- Cooperación con determinadas verificaciones.
- Comunicación de incidentes.
- Conservación de registros.
- Derecho de auditoría cuando corresponda.
- Consecuencias del incumplimiento.
- Posibilidad de terminación contractual en determinadas circunstancias.

Las cláusulas deben ser **proporcionales a la relación y al riesgo identificado**.

Cuando el socio no tiene controles antisoborno

Puede ocurrir que un proveedor o socio de negocio no disponga de un Sistema de Gestión Antisoborno propio. Esto **no significa automáticamente que la relación deba rechazarse**.

ISO 37001:2025 establece que, cuando corresponda por el nivel de riesgo, la organización debe determinar si el socio dispone de controles antisoborno adecuados y, cuando sea posible, exigir o promover la implementación de controles pertinentes. Cuando esto no sea posible, la situación debe considerarse en la evaluación del riesgo y en la manera en que la organización gestiona dicho riesgo.

Proveedores de bajo riesgo

No todos los proveedores necesitan una investigación exhaustiva. Por ejemplo, una organización puede considerar de **bajo riesgo** determinadas compras rutinarias, de bajo valor y sin contacto con funcionarios públicos. En estos casos pueden ser suficientes controles básicos, siempre que la evaluación de riesgos justifique esa clasificación.

Esto permite aplicar correctamente el principio de **proporcionalidad** y evita convertir la debida diligencia en un proceso burocrático innecesario.

Proveedores de alto riesgo

En cambio, puede ser necesario aplicar una debida diligencia reforzada cuando el proveedor:

- Participa en proyectos de gran valor.
- Actúa como intermediario.
- Tiene contacto frecuente con funcionarios públicos.
- Opera en actividades especialmente expuestas.
- Tiene una estructura de propiedad compleja.
- Presenta señales de alerta.
- Ha tenido antecedentes relevantes.
- Gestiona recursos importantes de la organización.

En estos casos, la organización debe obtener **información suficiente para comprender y gestionar adecuadamente el riesgo**.

Caso práctico: empresa minera

Una empresa minera necesita contratar un consultor para gestionar determinados trámites ante autoridades públicas.

La evaluación inicial determina que existe un **riesgo superior al bajo**.

La organización podría realizar las siguientes acciones:

Primero: verificar la existencia legal del consultor.

Segundo: identificar a sus propietarios y responsables.

Tercero: revisar su experiencia y capacidad profesional.

Cuarto: analizar posibles relaciones con funcionarios públicos.

Quinto: revisar información relevante sobre antecedentes y reputación.

Sexto: justificar la necesidad de contratar al consultor.

Séptimo: evaluar la razonabilidad de sus honorarios.

Octavo: incluir compromisos antisoborno en el contrato.

Noveno: establecer controles sobre los pagos.

Décimo: definir mecanismos de seguimiento durante la relación.

El objetivo no es crear obstáculos innecesarios, sino **reducir la posibilidad de que el tercero sea utilizado para realizar un soborno en nombre o beneficio de la organización**.

Documentación de la debida diligencia

La organización debe mantener **información documentada adecuada** sobre la debida diligencia realizada.

La documentación puede incluir:

- Identificación del tercero.
- Información recopilada.
- Fuentes consultadas.
- Evaluación del riesgo.
- Señales de alerta identificadas.
- Controles existentes.

- Decisión adoptada.
- Aprobaciones correspondientes.
- Medidas adicionales.
- Fecha de revisión.
- Próxima fecha de actualización.

La documentación proporciona **trazabilidad y evidencia** de que la organización tomó una decisión basada en un proceso definido.

Debida diligencia y protección de la organización

La debida diligencia no debe considerarse únicamente como una exigencia documental de ISO 37001. Bien aplicada, permite proteger a la organización frente a diferentes consecuencias:

Legales: exposición a investigaciones, sanciones o responsabilidades.

Financieras: pérdidas, contratos afectados o costos derivados de investigaciones.

Operativas: interrupciones de proyectos y relaciones comerciales.

Reputacionales: pérdida de confianza de clientes, autoridades, trabajadores e inversores.

De cumplimiento: incumplimiento de políticas internas o requisitos aplicables.

Por ello, **conocer adecuadamente a los socios de negocio es una medida de prevención**.

Errores frecuentes

Entre los errores más habituales en la debida diligencia se encuentran:

Aplicar el mismo nivel de revisión a todos los terceros. Esto genera procesos innecesariamente costosos y no refleja el principio de proporcionalidad.

Realizar la evaluación únicamente al inicio. Los riesgos pueden cambiar durante la relación.

Limitarse a comprobar la existencia legal. La existencia de una empresa no demuestra que el riesgo de soborno sea bajo.

Ignorar a los intermediarios. Los terceros que actúan en nombre de la organización pueden presentar una exposición significativa.

No investigar señales de alerta. Una señal relevante debe ser analizada antes de tomar una decisión.

No documentar la decisión. Sin evidencia, resulta difícil demostrar cómo se evaluó y gestionó el riesgo.

No establecer controles contractuales. La relación con un tercero de riesgo significativo debe contar con medidas apropiadas.

Relación con la evaluación de riesgos

La debida diligencia y la evaluación de riesgos están **directamente conectadas**.

La evaluación de riesgos determina:

qué relaciones presentan mayor exposición.

La debida diligencia determina:

qué información adicional necesitamos para comprender y gestionar esa exposición.

Los resultados de la debida diligencia pueden, a su vez, modificar la evaluación inicial del riesgo.

Por ejemplo, una relación inicialmente considerada de riesgo medio podría pasar a ser de riesgo alto si durante la investigación aparecen **vínculos relevantes con funcionarios públicos, antecedentes o irregularidades importantes**.

Principio de proporcionalidad

El concepto central de este apartado puede resumirse en una regla sencilla:

No todos los socios y proveedores deben ser investigados de la misma manera.

La organización debe aplicar medidas **razonables y proporcionales al riesgo de soborno**.

Esto permite construir un sistema que sea simultáneamente:

- Eficaz.
- Práctico.
- Proporcional.
- Documentado.
- Basado en riesgos.
- Integrado en los procesos normales de contratación.

ISO 37001:2025 está diseñado precisamente para que las medidas antisoborno se implementen de forma **razonable y proporcional**, en función de los riesgos identificados.

Metodología práctica

Una metodología básica para la debida diligencia puede organizarse de la siguiente manera:

1. Identificar al socio de negocio: determinar quién es, qué hace y qué relación tendrá con la organización.

2. Clasificar el riesgo: utilizar los resultados de la evaluación de riesgos de soborno.

3. Determinar el nivel de diligencia: establecer qué información debe recopilarse según el riesgo.

4. Recopilar información: obtener información suficiente y relevante.

5. Analizar señales de alerta: identificar circunstancias que requieran una revisión adicional.

6. Evaluar los resultados: determinar el nivel de riesgo real.

7. Adoptar una decisión: aprobar, aprobar con condiciones, solicitar medidas adicionales o no establecer/continuar la relación.

8. Implementar controles: establecer medidas contractuales, financieras y no financieras apropiadas.

9. Documentar: conservar evidencia de la evaluación y decisión.

10. Actualizar: revisar la información según la frecuencia definida y cuando aparezcan cambios relevantes.

Idea clave

La **debida diligencia de socios y proveedores es un proceso basado en riesgos**, no una simple comprobación administrativa.

ISO 37001:2025 exige que, cuando exista un riesgo de soborno superior al bajo en determinadas categorías de relaciones, transacciones, proyectos, actividades o posiciones, la organización obtenga información suficiente para evaluar la naturaleza y el alcance de ese riesgo. La debida diligencia debe actualizarse con una frecuencia definida para considerar cambios y nueva información. Además, cuando el riesgo asociado a un socio de negocio es superior al bajo, la organización debe establecer medidas adecuadas relacionadas con **controles antisoborno y compromisos del socio**, en la medida en que resulte posible y razonable. En definitiva, **conocer a quién contratamos, con quién hacemos negocios y quién actúa en nuestro nombre es una parte esencial de la prevención del soborno**. Una organización que identifica correctamente sus terceros, evalúa sus riesgos y aplica controles proporcionales está en mejores condiciones para prevenir tanto el soborno directo como el soborno indirecto.

En Perú, este enfoque es además plenamente compatible con la NTP-ISO 37001:2025, publicada por INACAL el 7 de agosto de 2025 como la segunda edición de la norma técnica peruana y equivalente a ISO 37001:2025.

4.3. Riesgos en minería, construcción y contrataciones con el Estado

Introducción

Los riesgos de soborno **no se presentan de la misma manera en todas las actividades económicas**. La naturaleza de las operaciones, el volumen de recursos involucrados, la relación con autoridades, el uso de contratistas y la complejidad de los proyectos pueden aumentar o reducir la exposición de una organización.

La **ISO 37001:2025** está diseñada para organizaciones de cualquier sector y contempla tanto el soborno directo como el indirecto, incluido el que puede producirse mediante socios de negocio. En el Perú, esta norma fue adoptada como **NTP-ISO 37001:2025**, segunda edición, publicada por INACAL el 7 de agosto de 2025.

En este contexto, **minería, construcción y contrataciones con el Estado** presentan situaciones que merecen especial atención dentro de una evaluación de riesgos antisoborno. Esto no significa que todas las empresas de estos sectores tengan un nivel de riesgo alto. El nivel debe determinarse mediante una evaluación específica de cada organización, proyecto y actividad.

¿Por qué estos sectores pueden presentar una exposición relevante?

Existen determinados factores que pueden incrementar la exposición al soborno:

- Elevado valor económico de determinados contratos y proyectos.
- Interacción frecuente con autoridades y entidades públicas.
- Necesidad de permisos, licencias, autorizaciones o certificaciones.
- Participación de numerosos contratistas y subcontratistas.
- Uso de intermediarios y consultores.
- Procesos de selección y contratación.
- Gestión de terrenos, concesiones o derechos.
- Supervisión y fiscalización de actividades.
- Pagos y operaciones de elevado valor.
- Proyectos desarrollados durante varios años.
- Participación de múltiples partes interesadas.

Estos factores no constituyen por sí mismos evidencia de soborno. Son elementos que deben ser considerados durante la identificación y evaluación del riesgo.

Riesgos específicos en el sector minero

La actividad minera puede involucrar numerosos procesos en los que existe interacción entre la empresa, proveedores, comunidades, contratistas y diferentes entidades públicas.

Dependiendo del proyecto, pueden existir riesgos relacionados con:

- Obtención y mantenimiento de permisos y autorizaciones.
- Trámites administrativos.
- Fiscalización y supervisión.
- Contratación de servicios especializados.

- Contratación de empresas locales.
- Adquisición de bienes y equipos.
- Transporte y logística.
- Gestión de terrenos.
- Relaciones con autoridades locales.
- Intermediarios.
- Consultores y representantes.
- Contratos de construcción y servicios.
- Gestión de proyectos de infraestructura.

Por ello, una empresa minera debería analizar **cada etapa relevante del proyecto**, en lugar de limitarse a evaluar el riesgo de soborno de manera general.

Permisos y autorizaciones

Uno de los escenarios que puede requerir especial atención es la interacción con autoridades durante procesos de autorización. Por ejemplo, una organización puede necesitar obtener determinadas autorizaciones antes de iniciar o ampliar una actividad.

El riesgo puede aparecer cuando una persona:

- Ofrece dinero para acelerar un trámite.
- Promete un beneficio personal a un funcionario.
- Utiliza un intermediario para realizar un pago indebido.
- Ofrece regalos con la intención de influir en una decisión.
- Solicita que un tercero realice una gestión irregular.

La organización debe distinguir claramente entre **una gestión administrativa legítima y una conducta destinada a influir indebidamente en una decisión**.

Intermediarios en minería

Los intermediarios pueden representar un riesgo particular cuando actúan en nombre de una empresa frente a autoridades. Por ejemplo, una empresa puede contratar a un consultor para realizar determinadas gestiones administrativas.

El riesgo aumenta cuando:

- El consultor tiene contacto directo con funcionarios.
- Sus funciones no están claramente definidas.
- Sus honorarios no están adecuadamente justificados.
- Solicita pagos a terceros.
- Se niega a proporcionar información.
- Tiene vínculos no declarados con funcionarios.
- Insiste en utilizar efectivo.
- Solicita evitar los procedimientos internos.

En estos casos, la **debida diligencia debe ser proporcional al riesgo identificado**.

Contratistas y subcontratistas en minería

Los grandes proyectos mineros pueden involucrar a numerosos contratistas y subcontratistas. La organización debe considerar que **el riesgo antisoborno no termina en sus propios trabajadores**.

Puede existir exposición a través de:

- Empresas contratistas.
- Empresas de transporte.
- Empresas de seguridad.
- Empresas de mantenimiento.
- Empresas de ingeniería.
- Consultores.
- Agentes.
- Proveedores especializados.
- Subcontratistas.

Por ello, la organización debe determinar cuáles de estas relaciones presentan un riesgo significativo y aplicar controles adecuados.

Riesgos en la selección de proveedores

Un posible escenario de riesgo consiste en favorecer indebidamente a un proveedor durante un proceso de selección.

Por ejemplo:

Un trabajador con autoridad para seleccionar proveedores recibe un beneficio personal a cambio de favorecer a una empresa determinada.

Los controles pueden incluir:

- Criterios objetivos de selección.
- Separación de funciones.
- Diferentes niveles de aprobación.
- Declaraciones de conflictos de interés.
- Evaluación de proveedores.
- Comparación de ofertas.
- Documentación de las decisiones.
- Controles sobre cambios contractuales.

El objetivo es reducir la posibilidad de que **una sola persona pueda manipular un proceso de contratación sin supervisión**.

Riesgos en construcción

El sector de la construcción también puede presentar diferentes escenarios de riesgo debido a la naturaleza de sus proyectos.

Entre los factores que pueden ser considerados se encuentran:

- Contratos de elevado valor.
- Licitaciones y concursos.
- Subcontratación.
- Certificaciones de avance.
- Valorizaciones.
- Modificaciones contractuales.
- Ampliaciones de plazo.
- Aprobación de trabajos adicionales.
- Inspecciones.
- Supervisión de obras.
- Recepción de trabajos.
- Adquisición de materiales.
- Uso de maquinaria y servicios.
- Interacción con autoridades.

La evaluación debe determinar **qué procesos presentan realmente mayor exposición**, evitando asumir que todos los proyectos tienen el mismo riesgo.

Valorizaciones y pagos

En proyectos de construcción puede existir una relación directa entre el avance físico de una obra y los pagos correspondientes.

Esto puede generar riesgos cuando una persona intenta:

- Inflar una valorización.
- Aprobar trabajos que no fueron ejecutados.
- Aceptar materiales que no cumplen las especificaciones.
- Autorizar pagos sin documentación suficiente.
- Manipular información sobre avances.
- Favorecer injustificadamente una ampliación contractual.

Los controles financieros y operativos deben estar diseñados para **reducir la posibilidad de que una sola persona controle todo el proceso**.

Modificaciones contractuales

Las modificaciones de contratos pueden representar un punto de atención en proyectos de construcción y otros proyectos de gran tamaño.

Una modificación puede afectar:

- Precio.
- Plazo.
- Alcance.
- Especificaciones.
- Cantidades.
- Condiciones de ejecución.

Por ello, los cambios importantes deben estar respaldados por **una justificación objetiva, documentación suficiente y las aprobaciones correspondientes**.

Riesgos relacionados con subcontratistas

Un contratista principal puede contratar a otras empresas para ejecutar parte de un proyecto. Esto puede generar un riesgo adicional porque la organización puede tener **varios niveles de terceros**.

Por ejemplo:

Empresa principal → contratista → subcontratista → proveedor.

Cuando existe una exposición significativa, la organización debe determinar hasta qué nivel necesita conocer y controlar estas relaciones.

El objetivo no es necesariamente investigar a todas las empresas de una cadena de suministro con la misma profundidad, sino **identificar dónde existe una exposición relevante al soborno y aplicar controles proporcionales**.

Contrataciones con el Estado en el Perú

Las contrataciones públicas constituyen un ámbito particularmente relevante para la gestión antisoborno porque implican procesos regulados, recursos públicos y participación de diferentes actores.

En el Perú, actualmente el marco general está establecido por la **Ley N.º 32069, Ley General de Contrataciones Públicas**, cuyo objeto es regular la contratación de bienes, servicios y obras y la participación de los actores involucrados en estos procesos. Su Reglamento fue aprobado mediante el **Decreto Supremo N.º 009-2025-EF**. Por tanto, las organizaciones que participan en contrataciones públicas deben considerar los riesgos de integridad y soborno dentro de sus procesos de cumplimiento.

Riesgos durante una contratación pública

Los riesgos pueden aparecer en diferentes etapas del proceso.

Por ejemplo:

Antes de la contratación: búsqueda de información privilegiada, conflictos de interés o intentos de influir indebidamente en las condiciones del proceso.

Durante la presentación de ofertas: coordinación indebida, manipulación de información o uso de intermediarios.

Durante la evaluación: intento de influir sobre personas encargadas de evaluar propuestas.

Durante la ejecución: pagos indebidos, modificaciones injustificadas, valorizaciones irregulares o aceptación de trabajos deficientes.

Durante la liquidación o cierre: alteración de información, aceptación de obligaciones no cumplidas o aprobación irregular de pagos.

La evaluación antisoborno debe considerar **todo el ciclo de la relación contractual**, no únicamente el momento de presentar una oferta.

Contacto con funcionarios públicos

Una organización que participa en contrataciones con el Estado puede mantener contacto con diferentes funcionarios y servidores públicos. Esto no constituye por sí mismo un riesgo de soborno.

El riesgo aparece cuando existe una **intención de obtener una ventaja indebida mediante una conducta prohibida**.

Por ello, la organización debe establecer reglas claras sobre:

- Reuniones con funcionarios.
- Regalos.
- Hospitalidad.
- Invitaciones.
- Gastos de representación.
- Comunicaciones.
- Intermediarios.
- Gestiones administrativas.

Regalos y hospitalidad

En sectores como minería, construcción y contratación pública, pueden existir relaciones comerciales que impliquen reuniones, eventos, viajes, comidas o invitaciones. La organización debe establecer **criterios claros para determinar cuándo un regalo o una atención es apropiada y cuándo puede generar un riesgo de soborno**.

Deben considerarse factores como:

- Valor.
- Frecuencia.
- Momento.
- Destinatario.
- Finalidad.
- Relación con una decisión pendiente.
- Transparencia.
- Autorizaciones internas.

Un regalo realizado durante un proceso de contratación pública puede presentar un riesgo muy diferente al de una atención comercial ordinaria de bajo valor realizada en circunstancias apropiadas.

Conflictos de interés

Los conflictos de interés constituyen un elemento especialmente importante en estos sectores. Por ejemplo, puede existir un conflicto cuando una persona responsable de seleccionar proveedores tiene una relación personal o económica con uno de los participantes.

La organización debe establecer mecanismos para:

- Identificar conflictos.
- Declararlos.
- Evaluarlos.
- Gestionarlos.
- Registrar las medidas adoptadas.

La **ISO 37001:2025 refuerza la consideración de los conflictos de interés dentro del sistema de gestión antisoborno**, como parte de las mejoras incorporadas en la nueva edición.

Riesgos financieros

Los controles financieros son particularmente importantes en proyectos de alto valor.

Entre las situaciones que pueden requerir atención se encuentran:

- Pagos sin documentación suficiente.
- Facturas falsas.
- Pagos en efectivo.
- Pagos a cuentas de terceros.
- Comisiones no justificadas.
- Honorarios desproporcionados.
- Anticipos sin controles adecuados.
- Pagos fraccionados para evitar autorizaciones.
- Registros contables incorrectos.

La organización debe establecer controles que permitan **autorizar, registrar y verificar adecuadamente las operaciones financieras**.

Riesgos no financieros

No todos los controles antisoborno son financieros. También pueden utilizarse controles no financieros, como:

- Procedimientos de contratación.
- Separación de funciones.
- Debida diligencia.
- Aprobaciones.
- Supervisión.
- Auditorías.
- Capacitación.
- Declaraciones de conflictos de interés.

- Controles sobre regalos y hospitalidad.
- Canal de denuncias.
- Evaluación de terceros.

Una gestión eficaz combina **controles financieros y no financieros**, de acuerdo con los riesgos identificados.

Riesgo de soborno indirecto

Uno de los aspectos más importantes para estos sectores es el **soborno indirecto**. Una organización puede no realizar directamente un pago indebido, pero podría existir un riesgo cuando una persona que actúa en su nombre o para su beneficio utiliza un tercero para realizarlo.

Por ejemplo:

Empresa → consultor → funcionario público.

Si el consultor utiliza un pago indebido para conseguir una autorización o ventaja para la empresa, la organización puede quedar expuesta a importantes consecuencias.

Por esta razón, la ISO 37001:2025 contempla expresamente el soborno **directo e indirecto**, incluido el realizado a través de terceros.

Señales de alerta

En minería, construcción y contrataciones públicas pueden aparecer diferentes señales que justifican una revisión adicional.

Entre ellas:

- Solicitud de pagos en efectivo.
- Uso de cuentas bancarias de terceros.
- Comisiones sin justificación clara.
- Honorarios extraordinariamente elevados.
- Intermediarios innecesarios.
- Relaciones no declaradas con funcionarios.
- Solicitudes para evitar procedimientos internos.
- Proveedores sin capacidad aparente para ejecutar el contrato.
- Modificaciones contractuales frecuentes sin justificación suficiente.
- Presiones para aprobar pagos rápidamente.
- Documentación incompleta.
- Conflictos de interés no declarados.

Una señal de alerta no equivale automáticamente a un acto de soborno. Debe ser analizada, documentada y, cuando corresponda, investigada.

Caso práctico: proyecto minero

Una empresa minera está desarrollando un proyecto que requiere contratar una empresa especializada para realizar determinadas gestiones.

Durante la evaluación se identifica que la empresa propuesta tiene:

- Contacto frecuente con autoridades.
- Honorarios superiores a los habituales.
- Una estructura de propiedad poco clara.
- Experiencia limitada para el servicio contratado.

La organización no debería limitarse a firmar el contrato. Puede realizar una **debida diligencia reforzada**, solicitar información adicional, justificar la necesidad de la contratación, analizar los honorarios y establecer controles específicos.

Si después de la evaluación el riesgo continúa siendo elevado, la dirección debe decidir si **acepta el riesgo con controles adicionales, modifica la estructura de la relación o no procede con la contratación**, de acuerdo con sus criterios internos.

Caso práctico: empresa constructora

Una empresa participa en un proyecto de construcción. Durante la ejecución, un responsable del proyecto solicita que se apruebe rápidamente una valorización adicional presentada por un contratista.

El procedimiento interno establece que las modificaciones deben ser revisadas y aprobadas por diferentes responsables. El responsable intenta evitar el procedimiento argumentando que existe “urgencia”.

Desde la perspectiva antisoborno, esta situación debería generar una **revisión del riesgo**, aunque no exista evidencia de que se haya producido un soborno. El control adecuado consiste en respetar el procedimiento y documentar la justificación de la modificación.

Caso práctico: contratación con el Estado

Una empresa participa en un procedimiento de contratación pública. Un intermediario afirma tener una relación cercana con personas vinculadas al proceso y ofrece “garantizar” que la empresa obtendrá el contrato a cambio de una comisión elevada.

Esta situación presenta varias señales de alerta:

- Uso de un intermediario.
- Promesa de influir en una decisión.
- Comisión elevada.
- Posible contacto indebido con funcionarios.
- Falta de justificación económica clara.

La organización debería **detener la operación y activar los procedimientos internos correspondientes**, antes de continuar con la relación.

Aplicación del enfoque basado en riesgos

La organización no debe comenzar preguntando:

"¿Qué controles debemos aplicar a minería?"

La pregunta correcta es:

"¿Qué riesgos de soborno existen en nuestras actividades mineras y qué controles son proporcionales a esos riesgos?"

El mismo principio se aplica a construcción y contrataciones públicas.

Dos empresas del mismo sector pueden presentar niveles de riesgo completamente diferentes debido a:

- Tamaño.
- Ubicación.
- Tipo de proyectos.
- Clientes.
- Intermediarios.
- Estructura organizativa.
- Nivel de interacción con autoridades.
- Valor de las operaciones.
- Controles existentes.

Por ello, **ISO 37001 no proporciona una matriz universal de riesgos para cada sector**. La organización debe desarrollar una evaluación adecuada a su propio contexto.

Relación con la Ley y el sistema de contratación pública

En el caso de organizaciones que participan en contrataciones públicas en Perú, el sistema antisoborno debe funcionar **complementariamente con el marco legal aplicable a las contrataciones públicas**.

La Ley N.º 32069 establece el marco general vigente de las contrataciones públicas, mientras que su Reglamento desarrolla las reglas correspondientes.

Por tanto, una empresa que participe en estos procesos debe diferenciar entre:

Cumplimiento legal: respetar las obligaciones establecidas por la legislación aplicable.

Cumplimiento antisoborno: establecer controles para prevenir, detectar y responder ante riesgos de soborno.

Sistema de gestión: integrar estos controles dentro de una estructura organizada, documentada y sometida a seguimiento y mejora.

Documentación de los riesgos sectoriales

La organización puede incorporar estos riesgos dentro de su **matriz general de riesgos de soborno**.

Por ejemplo:

Sector / actividad	Escenario de riesgo	Factor de exposición	Control posible
Minería	Soborno mediante intermediario	Contacto con autoridades	Debida diligencia
Minería	Pago indebido para acelerar autorización	Trámites administrativos	Aprobaciones y supervisión
Construcción	Aprobación irregular de valorizaciones	Alto valor contractual	Separación de funciones
Construcción	Favoritismo en selección de proveedor	Contratación	Criterios objetivos
Contratación pública	Influencia indebida sobre una decisión	Relación con funcionarios	Política y controles de interacción
Contratación pública	Pago indebido mediante tercero	Uso de intermediarios	Debida diligencia y controles contractuales

La matriz debe adaptarse a **las actividades reales de cada organización**.

Medidas preventivas recomendadas

Dependiendo del resultado de la evaluación, una organización puede establecer medidas como:

- Política antisoborno.
- Evaluación periódica de riesgos.
- Debida diligencia de terceros.
- Controles sobre intermediarios.
- Separación de funciones.
- Aprobaciones de operaciones.
- Controles financieros.
- Controles sobre regalos y hospitalidad.
- Gestión de conflictos de interés.
- Capacitación.
- Canal de denuncias.
- Investigación de incidentes.
- Auditorías internas.

- Seguimiento de terceros.
- Acciones correctivas.

La selección de estas medidas debe responder a **los riesgos identificados**, y no simplemente a una lista estándar de controles.

Idea clave

Minería, construcción y contrataciones con el Estado pueden presentar escenarios específicos de exposición al soborno, especialmente cuando existen proyectos de elevado valor, interacción con autoridades, intermediarios, contratistas, subcontratistas y procesos de contratación complejos.

Sin embargo, **no debe asumirse automáticamente que una actividad pertenece a una categoría de alto riesgo**. ISO 37001:2025 exige un enfoque basado en el contexto y en la evaluación de los riesgos reales de la organización. La norma puede aplicarse a organizaciones de cualquier sector y tamaño, y contempla tanto el soborno directo como el indirecto.

En Perú, este análisis debe considerar además el marco normativo vigente aplicable a cada actividad. En particular, las organizaciones que participan en contrataciones públicas deben tener presente la **Ley N.º 32069, Ley General de Contrataciones Públicas**, y su Reglamento aprobado mediante el **Decreto Supremo N.º 009-2025-EF**.

El objetivo final es que la organización pueda **identificar los escenarios de mayor exposición, aplicar controles proporcionales y mantener evidencia de las decisiones adoptadas**, integrando la prevención del soborno en la gestión cotidiana de sus proyectos y operaciones.

4.4. Gestión de regalos, hospitalidad y donaciones

Introducción

Los **regalos, la hospitalidad, las donaciones, los patrocinios y otros beneficios similares** pueden formar parte de las relaciones comerciales legítimas de una organización. Sin embargo, también pueden utilizarse para **influir indebidamente en una decisión, obtener una ventaja o encubrir un soborno**.

Por esta razón, la **ISO 37001:2025** incluye específicamente la gestión de **regalos, hospitalidad, donaciones y beneficios similares** dentro de los controles operativos del Sistema de Gestión Antisoborno, en el apartado 8.7.

La norma no establece que toda forma de regalo, hospitalidad o donación esté prohibida. El enfoque consiste en **identificar y gestionar el riesgo**, estableciendo controles razonables y proporcionales a las circunstancias.

¿Qué se entiende por regalos y beneficios?

En el contexto antisoborno, los beneficios pueden adoptar muchas formas.

Entre ellos pueden encontrarse:

- Regalos materiales.
- Comidas y cenas.
- Invitaciones a eventos.
- Entretenimiento.
- Viajes.
- Alojamiento.
- Entradas para espectáculos.
- Beneficios recreativos.
- Descuentos especiales.
- Préstamos o ventajas económicas.
- Donaciones.
- Patrocinios.
- Contribuciones a determinadas organizaciones.
- Otros beneficios similares.

El riesgo no depende únicamente del **valor económico** del beneficio. También deben considerarse **quién lo recibe, quién lo entrega, cuándo se entrega, por qué se entrega y qué decisión puede estar relacionada con él**.

¿Cuándo un regalo puede convertirse en un riesgo?

Un regalo puede generar un riesgo de soborno cuando tiene como finalidad **influir indebidamente en una decisión o conseguir una ventaja**. Por ejemplo, puede existir una situación de riesgo cuando una empresa entrega un regalo de valor considerable a una persona que está a punto de decidir si adjudica un contrato.

La situación puede resultar problemática incluso si el regalo se presenta como una simple cortesía comercial. La ISO 37001 reconoce precisamente que un tercero puede interpretar determinados regalos, beneficios u hospitalidad como un posible soborno **incluso cuando la persona que los ofrece o recibe no haya tenido esa intención**.

Por ello, la organización debe considerar también **cómo podría percibirse razonablemente la situación desde fuera**.

El contexto es fundamental

No existe una única cifra que permita determinar automáticamente si un regalo es apropiado o constituye soborno.

Deben analizarse diferentes circunstancias:

Valor: cuánto vale el beneficio.

Frecuencia: cuántas veces se ofrece al mismo destinatario.

Momento: si existe una decisión pendiente relacionada con la persona.

Destinatario: si es un funcionario público, cliente, proveedor, trabajador u otra persona.

Finalidad: por qué se ofrece.

Transparencia: si está registrado y autorizado.

Naturaleza: qué tipo de beneficio se proporciona.

Relación: qué vínculo existe entre quien entrega y quien recibe.

Percepción: cómo podría interpretar la situación un tercero independiente.

Por eso, **un beneficio de bajo valor no es automáticamente aceptable si se entrega con una finalidad indebida**.

Política de regalos y hospitalidad

Una organización que gestiona adecuadamente el riesgo debe establecer una **política clara sobre regalos, hospitalidad y beneficios similares**.

La política debería explicar:

- Qué tipos de beneficios están permitidos.
- Qué beneficios están prohibidos.
- Qué límites o criterios deben aplicarse.
- Cuándo se necesita autorización previa.
- Cuándo debe realizarse una declaración.
- Cómo deben registrarse los beneficios.
- Qué hacer cuando existe una duda.
- Qué hacer cuando una persona recibe un regalo inesperado.
- Cómo gestionar los beneficios ofrecidos a funcionarios públicos.
- Qué consecuencias pueden existir por incumplimiento.

La política debe ser **comprensible para los trabajadores y aplicable a las situaciones reales de la organización**.

Beneficios prohibidos

La organización puede establecer determinadas categorías de beneficios que estén **prohibidos independientemente de su valor**, especialmente cuando exista una finalidad claramente incompatible con la política antisoborno.

Por ejemplo:

- Dinero en efectivo entregado para influir en una decisión.
- Pagos personales destinados a obtener una ventaja.
- Beneficios vinculados a una decisión pendiente.
- Regalos destinados a conseguir un contrato.
- Beneficios ofrecidos a cambio de una autorización.
- Pagos encubiertos como regalos.
- Beneficios entregados para evitar un control o una sanción.

El objetivo es establecer una **línea clara entre una cortesía comercial legítima y una ventaja indebida**.

Regalos a funcionarios públicos

Las relaciones con **funcionarios públicos** requieren especial atención. Un regalo ofrecido a un funcionario puede ser interpretado como un intento de influir en una decisión, especialmente cuando:

- Existe un procedimiento administrativo en curso.
- Existe una licitación.
- Se está evaluando una autorización.
- Existe una inspección.
- Se está negociando un contrato.
- Se encuentra pendiente una decisión oficial.

Por esta razón, muchas organizaciones establecen **restricciones más estrictas para regalos y hospitalidad dirigidos a funcionarios públicos**.

En determinados casos, la política puede establecer que no se permite ningún beneficio, independientemente de su valor, cuando exista una relación directa con una decisión oficial.

Hospitalidad

La hospitalidad puede incluir comidas, eventos, viajes, alojamiento y actividades de entretenimiento. No toda hospitalidad es un soborno.

Por ejemplo, una reunión de trabajo acompañada de una comida razonable puede formar parte de una relación comercial legítima.

El riesgo aumenta cuando la hospitalidad:

- Es excesiva.
- Es frecuente.
- No tiene una finalidad comercial clara.
- Incluye gastos personales.
- Incluye viajes de placer.
- Se ofrece durante una decisión importante.
- Está dirigida a personas con poder de decisión.
- No está registrada.
- Se oculta deliberadamente.

Por ello, la organización debe establecer **criterios objetivos para determinar cuándo la hospitalidad es razonable y cuándo requiere autorización adicional**.

Viajes y alojamiento

Los viajes relacionados con actividades comerciales pueden presentar riesgos específicos. Por ejemplo, una empresa puede invitar a un representante de otra organización a visitar sus instalaciones.

La situación puede ser legítima si existe una finalidad empresarial clara. Sin embargo, deben analizarse aspectos como:

- Quién paga el viaje.
- Quién participa.
- Motivo del viaje.
- Duración.
- Nivel de gastos.
- Actividades realizadas.
- Participación de familiares.
- Existencia de una decisión pendiente.

Los gastos deben guardar una relación razonable con el propósito legítimo de la actividad.

Entretenimiento

Las entradas para eventos deportivos, espectáculos, conciertos u otras actividades pueden constituir hospitalidad.

La organización debe analizar especialmente:

- El valor de las entradas.
- La persona invitada.
- La finalidad.
- La frecuencia.
- La existencia de una decisión pendiente.
- Si participan representantes de la organización.
- Si existe una justificación comercial.

Una invitación puede presentar un riesgo considerablemente mayor cuando se realiza **inmediatamente antes de una decisión contractual importante**.

Frecuencia de los beneficios

Incluso beneficios de bajo valor pueden generar un riesgo cuando se entregan **repetidamente a la misma persona**. Por ejemplo, una organización puede establecer límites relacionados con:

- Valor individual.
- Valor acumulado.
- Número de beneficios durante un período.
- Tipo de destinatario.
- Situaciones especiales.

La frecuencia debe analizarse porque una sucesión de pequeños beneficios puede generar una situación muy diferente a un único beneficio ocasional.

Registro de regalos y hospitalidad

Un mecanismo práctico de control consiste en establecer un **registro de regalos y hospitalidad**.

El registro puede incluir:

- Fecha.
- Persona que ofrece el beneficio.
- Persona que lo recibe.
- Organización relacionada.
- Tipo de beneficio.
- Valor aproximado.
- Motivo.
- Decisión o autorización correspondiente.
- Resultado de la evaluación.

El registro permite aumentar la **transparencia y trazabilidad**. También permite detectar patrones que podrían pasar desapercibidos si cada beneficio se analiza de manera aislada.

Autorizaciones previas

Para determinadas categorías de regalos y hospitalidad, la organización puede establecer un requisito de **autorización previa**.

Por ejemplo, puede requerirse autorización cuando:

- El valor supera un determinado límite interno.
- El destinatario es un funcionario público.
- Existe una decisión contractual pendiente.
- El beneficio incluye viajes o alojamiento.
- Participan familiares.
- El beneficio es excepcional.
- Existe una señal de alerta.

La autorización debe estar basada en **criterios previamente definidos**, y no en una decisión improvisada.

Regalos recibidos

La política antisoborno debe explicar también **qué hacer cuando un trabajador recibe un regalo**. No todos los regalos pueden ser rechazados fácilmente. En determinadas situaciones, un tercero puede entregar un objeto promocional o una cortesía sin haberlo solicitado.

Por ello, la organización puede establecer diferentes medidas:

- Aceptación cuando el beneficio cumple los criterios internos.
- Declaración del regalo.
- Registro.

- Solicitud de autorización.
- Devolución.
- Entrega del regalo a la organización.
- Distribución conforme a un procedimiento interno.

Lo importante es que el trabajador **sepa qué hacer y no tenga que decidir individualmente cómo gestionar una situación potencialmente delicada**.

Donaciones

Las donaciones también pueden generar riesgos de soborno. Una organización puede realizar donaciones legítimas a:

- Organizaciones sociales.
- Instituciones educativas.
- Entidades sin fines de lucro.
- Comunidades.
- Proyectos sociales.
- Programas culturales.
- Organizaciones humanitarias.

Sin embargo, una donación puede convertirse en un riesgo cuando se utiliza **para obtener una ventaja indebida o influir en una decisión**. Por ejemplo, una organización podría realizar una donación a una entidad vinculada con una persona que tiene capacidad para tomar una decisión favorable para la empresa.

Por esta razón, las donaciones deben estar sujetas a **criterios de aprobación, evaluación y transparencia**.

Patrocinios

Los patrocinios también requieren controles. Un patrocinio puede ser perfectamente legítimo cuando tiene una finalidad empresarial, social, cultural o deportiva claramente definida.

Sin embargo, debe analizarse:

- Quién recibe los fondos.
- Quién controla la organización beneficiaria.
- Qué finalidad tiene el patrocinio.
- Qué beneficios recibe la empresa.
- Si existe una decisión pendiente.
- Si existen vínculos con funcionarios.
- Cómo se utilizarán los fondos.

La existencia de una actividad legítima no elimina automáticamente el riesgo de soborno.

Donaciones relacionadas con comunidades

En sectores como **minería y construcción**, las organizaciones pueden desarrollar programas sociales o realizar contribuciones a comunidades. Estas actividades pueden formar parte legítima de las relaciones con las partes interesadas.

Sin embargo, deben existir controles para evitar que una donación o contribución sea utilizada como mecanismo para:

- Obtener una autorización indebida.
- Influir sobre una autoridad.
- Favorecer una decisión.
- Ocultar un pago.
- Beneficiar indirectamente a una persona determinada.

La organización debe poder demostrar **el propósito legítimo y la transparencia de la contribución**.

Donaciones políticas

Las contribuciones relacionadas con actividades políticas presentan **riesgos particularmente sensibles** y deben gestionarse de acuerdo con las leyes aplicables y las políticas internas de la organización.

Cuando una organización permite determinadas contribuciones, debe establecer controles sobre:

- Autorización.
- Identificación del beneficiario.
- Finalidad.
- Cumplimiento legal.
- Registro contable.
- Transparencia.

Cuando la legislación o la política interna prohíba determinadas contribuciones, estas deben ser **rechazadas independientemente de la oportunidad comercial que pudiera existir**.

Separación entre donaciones y decisiones comerciales

Una regla práctica importante es evitar que una donación o patrocinio esté **condicionado a una decisión comercial o administrativa**. Por ejemplo, una situación de alto riesgo sería:

“Realizaremos una donación si se aprueba nuestra solicitud.”

La organización debe establecer una separación clara entre **las actividades legítimas de responsabilidad social y las decisiones comerciales o administrativas**.

Beneficios a través de terceros

El riesgo no desaparece cuando el beneficio se entrega mediante otra persona.

Por ejemplo:

Empresa → consultor → funcionario público

El consultor podría entregar un regalo, pagar una comida o realizar una contribución en beneficio de un funcionario. Por esta razón, la gestión de regalos, hospitalidad y donaciones debe estar integrada con los procesos de **debida diligencia y control de socios de negocio**.

ISO 37001:2025 contempla expresamente los riesgos de soborno directo e indirecto y los controles sobre socios de negocio.

Señales de alerta

Algunas situaciones pueden requerir una revisión adicional:

- El beneficiario solicita que el regalo no sea registrado.
- Se pide entregar el beneficio a un familiar.
- Existe una decisión pendiente.
- El valor es excesivamente elevado.
- Se repiten los beneficios.
- Se solicita dinero en lugar de un beneficio legítimo.
- La donación se dirige a una organización vinculada con un decisor.
- Se solicita realizar el pago a una cuenta personal.
- El intermediario no puede explicar la finalidad.
- Se intenta ocultar el verdadero beneficiario.
- Se pide registrar la operación de forma incorrecta.

Una señal de alerta no demuestra automáticamente la existencia de soborno, pero debe ser evaluada de acuerdo con los procedimientos internos.

Controles para las donaciones

Una organización puede establecer un procedimiento que incluya:

Solicitud: identificación del beneficiario y finalidad.

Evaluación: análisis del riesgo de soborno.

Debida diligencia: cuando corresponda por el nivel de riesgo.

Aprobación: autorización por el nivel correspondiente.

Pago: utilización de medios financieros trazables.

Registro: documentación de la operación.

Seguimiento: comprobación razonable del uso de los fondos cuando sea necesario.

Este proceso permite mantener **trazabilidad desde la solicitud hasta la utilización de la contribución**.

Controles financieros

Los regalos, hospitalidad y donaciones deben estar relacionados también con los **controles financieros de la organización**.

Algunos controles pueden incluir:

- Límites de autorización.
- Separación de funciones.
- Documentación de gastos.
- Comprobantes.
- Registro contable adecuado.
- Prohibición de determinados pagos.
- Revisión de operaciones excepcionales.
- Supervisión de gastos.
- Auditoría.

La finalidad es evitar que un beneficio pueda ocultarse dentro de una operación financiera aparentemente legítima.

Documentación

La organización debe mantener documentación suficiente para demostrar **cómo se gestionaron las situaciones relevantes**.

Dependiendo del caso, puede conservar:

- Solicitudes.
- Aprobaciones.
- Registros de regalos.
- Justificaciones.
- Facturas.
- Comprobantes.
- Información del beneficiario.
- Evaluaciones de riesgo.
- Resultados de la debida diligencia.
    - Comunicaciones relevantes.

La documentación permite demostrar que la decisión fue tomada de acuerdo con **los controles establecidos por la organización**.

Capacitación del personal

La política de regalos, hospitalidad y donaciones debe ser conocida por los trabajadores.

La capacitación debe explicar, de forma práctica:

- Qué está permitido.
- Qué está prohibido.
- Cuándo solicitar autorización.
- Cómo registrar un beneficio.
- Qué hacer ante una situación dudosa.
- Cómo actuar frente a funcionarios públicos.
- Cómo comunicar una preocupación.

La capacitación es especialmente importante para trabajadores que mantienen contacto frecuente con:

- Clientes.
- Proveedores.
- Funcionarios públicos.
- Contratistas.
- Intermediarios.
- Socios de negocio.

ISO 37001:2025 incluye capacitación y concienciación como componentes del Sistema de Gestión Antisoborno.

Ejemplo práctico: regalo a un funcionario

Una empresa está esperando una autorización importante. Un representante comercial propone entregar un regalo de alto valor al funcionario encargado del procedimiento.

Aunque el representante diga que se trata de una “atención comercial”, existen varios factores de riesgo:

Existe una decisión pendiente.

El destinatario tiene capacidad de decisión.

El valor es elevado.

Existe una relación directa entre el beneficio y la decisión.

La organización debería **rechazar la operación y aplicar sus procedimientos internos**, ya que la situación presenta un riesgo evidente de influencia indebida.

Ejemplo práctico: invitación empresarial

Una empresa invita a un proveedor a una comida de trabajo para analizar las condiciones de un proyecto.

La invitación tiene:

- Finalidad empresarial clara.
- Valor razonable.
- Participación de representantes de ambas organizaciones.
- Registro adecuado.
- Ausencia de una decisión que se pretenda influenciar.

En principio, podría tratarse de una hospitalidad comercial legítima, **siempre que sea coherente con las políticas internas y las circunstancias concretas**.

Ejemplo práctico: donación

Una empresa recibe una solicitud para realizar una donación a una organización vinculada con una persona que participa en la evaluación de un proyecto.

Antes de aprobarla, la organización debería analizar:

- Quién controla la organización beneficiaria.
- Qué relación existe con el decisor.
- Cuál es la finalidad de la donación.
- Si existe una decisión pendiente.
- Si la contribución está permitida.
- Qué controles deben aplicarse.

Si la evaluación determina que la donación puede ser percibida razonablemente como un mecanismo para influir en la decisión, **la organización debe aplicar medidas adecuadas o rechazarla**.

Enfoque basado en riesgos

La gestión de regalos, hospitalidad y donaciones debe seguir el mismo principio que el resto del Sistema de Gestión Antisoborno:

identificar el riesgo → evaluar las circunstancias → aplicar controles proporcionales → documentar → supervisar.

Esto evita dos extremos. El primero consiste en **permitir prácticamente cualquier beneficio**, lo que puede generar una exposición innecesaria.

El segundo consiste en **prohibir absolutamente todas las relaciones comerciales**, lo que puede ser poco práctico y no necesariamente necesario.

El enfoque de ISO 37001 busca establecer **medidas razonables y proporcionales al riesgo**.

Revisión y actualización

La organización debe revisar periódicamente sus controles y considerar los cambios en sus actividades.

Puede ser necesario actualizar la política cuando:

- Se identifican nuevos riesgos.
- Cambia la legislación aplicable.
- Se modifican las actividades.
- Se ingresa a nuevos mercados.
- Aumenta la interacción con funcionarios.
- Se producen incidentes.
- Los controles existentes demuestran ser insuficientes.
- Cambian los tipos de beneficios utilizados por la organización.

La mejora continua permite que **la política no se convierta en un documento estático**, sino en una herramienta de gestión.

Metodología práctica

Una organización puede gestionar los regalos, la hospitalidad y las donaciones mediante el siguiente proceso:

1. Definir las reglas: establecer qué beneficios están permitidos, restringidos o prohibidos.

2. Establecer criterios: determinar límites y factores de riesgo.

3. Identificar situaciones especiales: funcionarios públicos, decisiones pendientes, intermediarios y otros escenarios sensibles.

4. Solicitar autorización: cuando el nivel de riesgo o el valor lo requiera.

5. Registrar: documentar los beneficios y decisiones relevantes.

6. Evaluar excepciones: analizar situaciones que no estén claramente contempladas.

7. Controlar los pagos: garantizar trazabilidad financiera.

8. Capacitar: asegurar que los trabajadores conozcan las reglas.

9. Supervisar: identificar patrones o situaciones inusuales.

10. Revisar y mejorar: actualizar los controles según los resultados obtenidos.

Idea clave

Los regalos, la hospitalidad, las donaciones y otros beneficios no están automáticamente prohibidos por ISO 37001:2025. El objetivo de la norma es que la organización establezca controles adecuados para prevenir que estos beneficios sean utilizados como instrumentos de soborno o puedan ser razonablemente percibidos como tales. El apartado **8.7 de ISO 37001:2025** contempla específicamente esta materia dentro de los controles operativos.

La organización debe considerar **el valor, la frecuencia, el destinatario, la finalidad, el momento, la relación existente y las circunstancias de cada caso**. En

especial, deben aplicarse controles reforzados cuando exista relación con funcionarios públicos, procesos de contratación, autorizaciones, inspecciones o decisiones comerciales relevantes.

La regla fundamental es la proporcionalidad: cuanto mayor sea el riesgo de que un beneficio pueda influir indebidamente en una decisión, mayor debe ser el nivel de control, autorización, documentación y supervisión.

En el Perú, este enfoque forma parte de la **NTP-ISO 37001:2025**, equivalente nacional de ISO 37001:2025 y vigente desde su publicación por INACAL el **7 de agosto de 2025**.

5. Controles Operativos y Financieros

5.1. Controles financieros y comerciales

Introducción

Los **controles financieros y comerciales** constituyen una parte fundamental del Sistema de Gestión Antisoborno, porque permiten reducir la posibilidad de que recursos económicos, operaciones comerciales o decisiones internas sean utilizados para facilitar, ocultar o ejecutar un soborno.

La **ISO 37001:2025**, actualmente vigente como segunda edición internacional, establece en su capítulo 8 la necesidad de implementar **controles financieros y controles no financieros** para gestionar el riesgo de soborno. En el Perú, la norma correspondiente es la **NTP-ISO 37001:2025**, publicada por INACAL el 7 de agosto de 2025.

Los controles financieros se relacionan principalmente con la forma en que la organización **autoriza, ejecuta, registra y supervisa sus operaciones económicas**. Los controles comerciales y no financieros, por su parte, abarcan áreas como compras, ventas, operaciones, recursos humanos, actividades legales y relaciones con terceros.

¿Qué son los controles financieros?

Los **controles financieros** son procedimientos y mecanismos destinados a garantizar que las operaciones económicas de la organización sean realizadas de manera adecuada, autorizada, transparente y correctamente registradas.

Desde la perspectiva antisoborno, su finalidad no consiste únicamente en evitar errores contables. También buscan **reducir la posibilidad de que un pago indebido pueda realizarse o esconderse dentro de una operación aparentemente legítima**.

Entre las operaciones que pueden estar sujetas a estos controles se encuentran:

- Pagos a proveedores.
- Transferencias bancarias.
- Anticipos.
- Reembolsos de gastos.
- Comisiones.
- Honorarios.
- Pagos a consultores.
- Gastos de representación.
- Donaciones.
- Patrocinios.
- Compras.
- Contratos de servicios.
- Operaciones en efectivo.

Importancia de la trazabilidad

Una operación financiera debe poder ser **rastreada desde su origen hasta su registro final**.

Esto significa que debería ser posible responder preguntas como:

¿Quién solicitó el pago?

¿Por qué se realizó?

¿Quién lo autorizó?

¿Quién recibió el dinero?

¿Qué documento respalda la operación?

¿Cómo fue registrado contablemente?

La trazabilidad dificulta que un pago indebido pueda ocultarse mediante conceptos ambiguos, documentación falsa o registros incompletos.

Separación de funciones

Uno de los controles financieros más importantes es la **separación de funciones**. La misma persona no debería concentrar, sin controles adicionales, todas las etapas de una operación.

Por ejemplo, debe evitarse una situación en la que una sola persona pueda:

solicitar un servicio → aprobarlo → confirmar que fue realizado → autorizar el pago → registrar la operación.

Separar estas funciones permite introducir **controles cruzados** y reducir las posibilidades de abuso. La orientación asociada a ISO 37001 tradicionalmente contempla precisamente la separación entre la iniciación y aprobación de pagos como una medida para reducir el riesgo de soborno.

Niveles de autorización

Las organizaciones pueden establecer **diferentes niveles de autoridad dependiendo del importe y del nivel de riesgo de la operación**.

Por ejemplo:

- Gastos menores: aprobación del responsable del área.
- Operaciones de importe medio: aprobación adicional.
- Operaciones de alto valor: aprobación de un nivel superior.
- Operaciones excepcionales: revisión específica.

La finalidad es evitar que una persona pueda aprobar por sí sola operaciones que excedan sus competencias.

Cuanto mayor sea el importe o el riesgo de una operación, mayor debería ser el nivel de control requerido.

Documentación de los pagos

Los pagos deben contar con **documentación suficiente que permita justificar la operación**.

Dependiendo de la naturaleza del gasto, puede incluir:

- Contrato.
- Orden de compra.
- Factura.
- Informe o evidencia del servicio.
- Aprobación correspondiente.
- Comprobante de entrega.
- Documento de recepción.
- Registro contable.

La documentación debe permitir demostrar que **el bien o servicio realmente fue solicitado, recibido y pagado de acuerdo con las condiciones aprobadas**.

Control sobre proveedores

Los proveedores pueden constituir una vía de exposición al soborno, especialmente cuando realizan actividades en nombre de la organización o mantienen contacto con funcionarios públicos.

Por ello, los controles financieros deben complementarse con la **debida diligencia de socios de negocio**, especialmente cuando el nivel de riesgo lo justifique.

Antes de realizar determinados pagos, la organización puede verificar:

- Identidad del proveedor.
- Existencia legal.
- Cuenta bancaria.
- Titularidad de la cuenta.
- Condiciones contractuales.
- Servicios realmente prestados.
- Facturación.
- Personas autorizadas.
- Posibles conflictos de interés.

Esto ayuda a evitar pagos a **proveedores ficticios, cuentas no autorizadas o terceros que no correspondan a la relación contractual**.

Control de cuentas bancarias

Las organizaciones deben establecer procedimientos para controlar las cuentas bancarias utilizadas para realizar y recibir pagos. Una situación de riesgo puede presentarse cuando un proveedor solicita que el pago sea realizado a:

una cuenta bancaria perteneciente a una persona distinta del proveedor contratado.

Este tipo de modificación no significa automáticamente que exista un soborno, pero debería generar una **revisión adicional y una justificación documentada**. Las modificaciones de cuentas bancarias deben estar sujetas a procedimientos de verificación y autorización.

Uso de efectivo

El uso de efectivo puede dificultar la trazabilidad de determinadas operaciones y, dependiendo del contexto, aumentar el riesgo de utilización indebida.

Por ello, la organización puede establecer:

- Límites para pagos en efectivo.
- Autorizaciones especiales.
- Documentación obligatoria.
- Conciliaciones de caja.
- Revisión periódica.
- Prohibición de determinadas operaciones en efectivo.

Cuando sea posible y apropiado, los **medios de pago trazables** facilitan la supervisión y el control.

Comisiones y honorarios

Las comisiones y honorarios pagados a agentes, consultores, intermediarios u otros terceros deben estar **justificados por servicios reales y legítimos**.

Una organización debe prestar especial atención cuando:

- La comisión es desproporcionada.
- El servicio no está claramente definido.
- El tercero no demuestra capacidad para realizarlo.
- El pago se solicita en efectivo.
- Se solicita pagar a una cuenta de otro país sin justificación.
- El tercero tiene vínculos con funcionarios.
- El pago está condicionado a la obtención de una decisión favorable.

Una comisión comercial legítima debe poder explicarse, documentarse y justificarse económicamente.

Registros contables precisos

Los registros contables deben reflejar correctamente la naturaleza de las operaciones. No es adecuado registrar un pago destinado a una finalidad determinada bajo un concepto diferente con el objetivo de ocultar su verdadera naturaleza.

Por ejemplo, un pago realizado como beneficio personal no debería registrarse falsamente como:

“servicios de consultoría”,
“gastos administrativos” o
“gastos comerciales”.

La organización debe procurar que las operaciones sean **registradas de manera clara, completa y exacta**.

Controles comerciales

Los controles antisoborno no se limitan al departamento financiero. La ISO 37001:2025 contempla también **controles no financieros** en áreas como adquisiciones, operaciones, ventas, actividades comerciales, recursos humanos, asuntos legales, fusiones y adquisiciones y actividades regulatorias.

Estos controles son importantes porque muchas situaciones de riesgo se originan **antes de que se produzca el pago**.

Controles en compras

El proceso de compras debe evitar que una persona pueda seleccionar arbitrariamente a un proveedor a cambio de un beneficio personal.

Algunos mecanismos pueden incluir:

- Criterios objetivos de selección.
- Solicitud de varias cotizaciones cuando corresponda.
- Evaluación de proveedores.
- Declaración de conflictos de interés.
- Separación entre selección y aprobación.
- Documentación de la decisión.
- Control sobre modificaciones contractuales.

El objetivo es que la selección pueda ser **explicada y defendida mediante criterios objetivos**.

Controles en ventas

Los riesgos antisoborno también pueden aparecer en el área comercial. Por ejemplo, un trabajador puede ofrecer un beneficio indebido a una persona que representa a un cliente con el objetivo de conseguir un contrato.

Por ello, la organización puede establecer controles relacionados con:

- Descuentos excepcionales.
- Comisiones.
- Contratos con intermediarios.
- Representantes comerciales.
- Gastos de representación.
- Regalos y hospitalidad.
- Condiciones comerciales extraordinarias.

La presión por alcanzar objetivos comerciales no justifica una conducta contraria a la política antisoborno.

Descuentos y condiciones especiales

Los descuentos comerciales pueden ser legítimos, pero deberían estar respaldados por **criterios definidos y documentados**.

Una situación de riesgo puede aparecer cuando un trabajador ofrece a un cliente una condición comercial excepcional y utiliza parte del beneficio para favorecer personalmente a una persona relacionada con la operación.

Por ello, los descuentos importantes o excepcionales pueden requerir:

- Justificación comercial.
- Aprobación.
- Registro.
- Revisión independiente.

Contratos comerciales

Los contratos con clientes, proveedores, consultores y otros socios de negocio deben establecer claramente:

- Objeto del servicio.
- Obligaciones de las partes.
- Precio.
- Forma de pago.
- Condiciones de ejecución.
- Responsabilidades.
- Requisitos de cumplimiento.
- Cuando corresponda, compromisos antisoborno.

Los contratos constituyen una herramienta importante porque permiten **formalizar las expectativas de comportamiento y establecer condiciones verificables**.

Pagos por servicios realmente prestados

Antes de efectuar un pago, la organización debe poder comprobar razonablemente que **el servicio o producto contratado realmente fue entregado**. Por ejemplo, si se

contrata a un consultor por un servicio específico, debería existir evidencia suficiente de que el trabajo fue realizado.

Esto permite reducir el riesgo de utilizar **servicios ficticios como mecanismo para justificar pagos indebidos**.

Anticipos

Los anticipos pueden ser necesarios en determinadas operaciones comerciales, pero deben gestionarse adecuadamente.

La organización puede establecer:

- Justificación del anticipo.
- Aprobación previa.
- Límites.
- Condiciones contractuales.
- Registro.
- Rendición posterior.
- Conciliación.

Un anticipo que permanece indefinidamente sin justificación o liquidación puede constituir una **señal de alerta**.

Gastos de representación

Los gastos de representación deben tener una finalidad comercial legítima y estar sujetos a reglas claras.

La organización puede establecer requisitos relacionados con:

- Persona beneficiaria.
- Finalidad.
- Fecha.
- Lugar.
- Participantes.
- Importe.
- Comprobantes.
- Autorización.

Los gastos especialmente elevados o inusuales deberían estar sujetos a **revisión adicional**.

Donaciones y patrocinios

Como se estudió en el punto anterior, las donaciones y patrocinios también pueden tener implicaciones financieras.

Por ello, deben contar con:

- Finalidad legítima.
- Beneficiario identificado.
- Aprobación.
- Documentación.
- Registro financiero.
- Evaluación de riesgos cuando corresponda.

La organización debe evitar que una donación sea utilizada para **canalizar indirectamente un beneficio hacia una persona que participa en una decisión relevante**.

Controles sobre operaciones excepcionales

Las operaciones que se apartan significativamente de los procedimientos habituales deben recibir **una atención proporcional a su nivel de riesgo**.

Entre ellas pueden encontrarse:

- Pagos extraordinarios.
- Contratos urgentes.
- Cambios importantes de proveedores.
- Modificaciones de precios.
- Comisiones excepcionales.
- Descuentos extraordinarios.
- Pagos a terceros.
- Operaciones fuera del procedimiento habitual.

Una excepción puede ser legítima, pero debe existir **una justificación documentada y una aprobación adecuada**.

Señales de alerta financieras

Algunas situaciones que pueden requerir una revisión adicional son:

- Pagos sin documentación suficiente.
- Facturas con descripciones excesivamente genéricas.
- Pagos a cuentas de terceros.
- Solicitudes de efectivo.
- Comisiones desproporcionadas.
- Cambios frecuentes de cuentas bancarias.
- Proveedores sin capacidad aparente.
- Pagos urgentes sin justificación.
- Fraccionamiento de operaciones.
- Servicios que no pueden demostrarse.
- Registros contables poco claros.
- Gastos comerciales inusualmente elevados.

Una señal de alerta no demuestra por sí misma que haya existido soborno. Su función es indicar que puede ser necesario realizar una revisión adicional.

Controles preventivos y controles detectivos

Los controles pueden cumplir diferentes funciones. Los **controles preventivos** buscan impedir que una operación indebida ocurra.

Por ejemplo:

- Autorización previa.
- Separación de funciones.
- Límites de gasto.
- Debida diligencia.
- Aprobación de proveedores.

Los **controles detectivos** buscan identificar operaciones problemáticas después o durante su ejecución.

Por ejemplo:

- Conciliaciones.
- Auditorías.
- Revisiones financieras.
- Análisis de operaciones inusuales.
- Revisiones de registros.
- Investigaciones.

Un sistema eficaz necesita **una combinación de controles preventivos y detectivos**.

Controles proporcionales al riesgo

No todas las organizaciones necesitan exactamente los mismos controles. Una empresa pequeña con pocas operaciones puede utilizar procedimientos relativamente sencillos.

Una organización con:

- Grandes proyectos.
- Numerosos proveedores.
- Operaciones internacionales.
- Contrataciones públicas.
- Intermediarios.
- Grandes volúmenes financieros.

puede necesitar controles considerablemente más robustos.

La ISO 37001 está diseñada para organizaciones de diferentes tamaños y sectores, por lo que **los controles deben adaptarse al contexto y al nivel de riesgo de la organización**.

Integración entre controles financieros y comerciales

Los controles financieros y comerciales no deben funcionar como sistemas aislados. Por ejemplo:

Compras selecciona un proveedor.

Área técnica confirma que el servicio fue realizado.

Finanzas verifica la documentación y procesa el pago.

Responsable autorizado aprueba la operación.

Contabilidad registra correctamente la transacción.

Esta interacción genera diferentes puntos de control y reduce la posibilidad de que una sola persona pueda manipular todo el proceso.

Caso práctico: proveedor ficticio

Una empresa recibe una factura de un supuesto consultor por un servicio de asesoría. El área financiera observa que:

- El servicio está descrito de forma muy general.
- No existe un informe del trabajo realizado.
- El importe es elevado.
- El proveedor fue incorporado recientemente.
- La cuenta bancaria pertenece a un país diferente al habitual.

Ninguna de estas circunstancias demuestra automáticamente un soborno. Sin embargo, en conjunto constituyen **señales de alerta que justifican una revisión antes de efectuar el pago**.

Caso práctico: pago a un tercero

Un proveedor solicita que una factura sea pagada a la cuenta bancaria de otra empresa.

La organización debe solicitar una explicación y verificar:

- Motivo del cambio.
- Relación entre las empresas.
- Titularidad de la cuenta.
- Autorización contractual.
- Documentación correspondiente.

Si la explicación no resulta razonable, **el pago debe quedar sujeto a una revisión adicional**.

Caso práctico: comisión comercial

Un intermediario solicita una comisión del 20 % del valor de un contrato y afirma que tiene “contactos especiales” que permitirán obtenerlo.

La organización debería considerar diversos factores:

El porcentaje es elevado.

La finalidad del servicio no está claramente definida.

Se mencionan contactos especiales.

Existe una posible relación con una decisión contractual.

La situación debería ser sometida a **debida diligencia y evaluación de riesgo antes de establecer la relación o efectuar cualquier pago**.

Auditoría de los controles financieros

Los controles financieros deben ser revisados periódicamente para comprobar si realmente funcionan.

La organización puede analizar:

- Operaciones excepcionales.
- Pagos de alto valor.
- Proveedores nuevos.
- Comisiones.
- Donaciones.
- Gastos de representación.
- Reembolsos.
- Cambios de cuentas.
- Operaciones con terceros.

La revisión puede identificar **debilidades del sistema antes de que se conviertan en incidentes importantes**.

Mejora continua

Cuando un control demuestra ser insuficiente, la organización debe analizar qué ocurrió y determinar si es necesario modificar el procedimiento. Por ejemplo, si se detecta que varios pagos importantes fueron aprobados sin una revisión adecuada, puede ser necesario:

- Modificar los niveles de autorización.
- Separar funciones.
- Incorporar una segunda revisión.
- Mejorar la documentación.
- Capacitar al personal.

- Realizar controles periódicos.

La gestión antisoborno debe mantenerse como **un sistema vivo y sujeto a mejora continua**, no como un conjunto estático de documentos. ISO 37001:2025 establece precisamente un marco para establecer, implementar, mantener, revisar y mejorar el sistema de gestión antisoborno.

Idea clave

Los **controles financieros y comerciales** constituyen una de las principales barreras contra el soborno porque permiten controlar tanto **el movimiento de los recursos como las decisiones que preceden a una operación financiera**.

Un sistema adecuado debe procurar que:

Las operaciones tengan una finalidad legítima.

Las personas responsables estén claramente identificadas.

Las funciones estén adecuadamente separadas.

Los pagos cuenten con autorización.

Los servicios y productos puedan ser verificados.

Los registros contables sean exactos y transparentes.

Las operaciones excepcionales sean revisadas.

Los terceros sean evaluados de acuerdo con su nivel de riesgo.

Los controles sean supervisados y mejorados periódicamente.

La **ISO 37001:2025 establece expresamente los controles financieros en el apartado 8.3 y los controles no financieros en el apartado 8.4**, mientras que la NTP-ISO 37001:2025 constituye la adopción vigente de esta norma en el Perú.

El objetivo final no es crear una burocracia financiera innecesaria, sino conseguir que **los recursos de la organización no puedan utilizarse fácilmente para realizar, facilitar u ocultar un soborno**, manteniendo al mismo tiempo controles proporcionales al tamaño, actividad y nivel de riesgo de la organización.

5.2. Aprobación de pagos y transacciones

Introducción

La **aprobación de pagos y transacciones** es un elemento esencial de los controles financieros de un Sistema de Gestión Antisoborno. Su finalidad es garantizar que las

operaciones económicas de la organización sean **legítimas, justificadas, autorizadas, correctamente documentadas y trazables**.

La **ISO 37001:2025** establece controles financieros como parte de los mecanismos destinados a prevenir, detectar y responder al soborno. La norma reconoce que los riesgos pueden producirse tanto de manera directa como indirecta, incluso mediante terceros que actúan en nombre o para beneficio de la organización.

En el Perú, la referencia nacional vigente es la **NTP-ISO 37001:2025**, publicada por INACAL el 7 de agosto de 2025, que reemplazó a la edición anterior NTP-ISO 37001:2017.

Objetivo de la aprobación de pagos

El objetivo principal es asegurar que **ningún pago pueda realizarse únicamente por decisión de una persona sin los controles correspondientes**.

Antes de efectuar una transacción, la organización debería poder determinar:

- **Qué se está pagando.**
- **Por qué se está pagando.**
- **A quién se está pagando.**
- **Quién solicitó la operación.**
- **Quién verificó que la operación es legítima.**
- **Quién autorizó el pago.**
- **Qué documentación respalda la operación.**
- **Cómo será registrada contablemente.**

Este proceso permite reducir la posibilidad de que un pago legítimo sea utilizado como mecanismo para **realizar, facilitar o esconder un soborno**.

Principio de autorización

Una operación financiera debe ser aprobada por una persona que tenga **autoridad suficiente para hacerlo**.

La autoridad debe estar definida previamente mediante políticas, procedimientos, matrices de autorización u otros mecanismos internos.

Por ejemplo, una organización puede establecer diferentes niveles de aprobación según:

- Importe.
- Tipo de operación.
- Área responsable.
- Nivel de riesgo.
- Naturaleza del proveedor.
- Tipo de contrato.
- Relación con funcionarios públicos.
- Carácter excepcional de la operación.

La persona que realiza el pago no debería poder decidir por sí sola si el pago es legítimo y aprobarlo sin ningún control independiente.

Separación de funciones

Uno de los principios fundamentales consiste en **separar las funciones críticas de una transacción**.

Por ejemplo:

Solicitar → revisar → aprobar → ejecutar → registrar → conciliar.

Estas funciones pueden estar distribuidas entre diferentes personas o áreas, dependiendo del tamaño y complejidad de la organización. La finalidad es evitar que una sola persona pueda controlar todo el proceso y modificarlo sin supervisión.

Ejemplo de separación de funciones

Una empresa contrata a un proveedor para realizar un servicio. El proceso podría funcionar de la siguiente manera:

Área solicitante: identifica la necesidad.

Área de compras: selecciona o gestiona al proveedor.

Área responsable del servicio: confirma que el trabajo fue realizado.

Responsable autorizado: aprueba la factura.

Área financiera: ejecuta el pago.

Contabilidad: registra la operación.

Tesorería o responsable correspondiente: realiza las conciliaciones y controles posteriores.

Este modelo crea **diferentes puntos de verificación**.

Verificación antes del pago

Antes de aprobar una transacción, debe verificarse que la documentación sea suficiente y coherente.

Dependiendo del tipo de operación, puede revisarse:

- Contrato.
- Orden de compra.
- Factura.
- Informe del servicio.

- Acta de recepción.
- Evidencia de entrega.
- Condiciones de pago.
- Identidad del proveedor.
- Cuenta bancaria.
- Aprobaciones requeridas.

El objetivo no es generar documentación innecesaria, sino garantizar que **exista evidencia suficiente para justificar la transacción**.

Confirmación del servicio o producto

Una de las verificaciones más importantes consiste en confirmar que **el bien o servicio realmente fue recibido**. Por ejemplo, si una empresa recibe una factura de S/ 50 000 por servicios de consultoría, la aprobación no debería basarse únicamente en la existencia de la factura.

Debe existir evidencia razonable de:

- Qué servicio se contrató.
- Qué trabajo se realizó.
- Quién lo recibió.
- Cuándo se realizó.
- Qué importe correspondía pagar.

Esto ayuda a prevenir el uso de **facturas por servicios inexistentes** como mecanismo para transferir fondos.

Pagos a proveedores

Los pagos a proveedores deben realizarse de acuerdo con las condiciones establecidas en el contrato y en los procedimientos internos.

Debe prestarse especial atención cuando se solicita:

- Cambiar la cuenta bancaria.
- Cambiar el beneficiario.
- Pagar a una empresa diferente.
- Pagar a una persona natural.
- Realizar el pago en efectivo.
- Dividir el pago.
- Acelerar excepcionalmente una transferencia.

Estas situaciones **no constituyen automáticamente un soborno**, pero pueden justificar una verificación adicional.

Cambios de cuentas bancarias

Los cambios de cuentas bancarias son especialmente importantes desde el punto de vista del control financiero. Por ejemplo, un proveedor solicita mediante correo electrónico

que todas las futuras facturas sean pagadas a una nueva cuenta bancaria perteneciente a otra empresa. La organización debería aplicar un procedimiento de verificación antes de aceptar el cambio.

Puede comprobar:

- Que la solicitud proviene realmente del proveedor.
- Identidad del titular de la cuenta.
- Relación entre la cuenta y el proveedor.
- Motivo del cambio.
- Autorización correspondiente.
- Información contractual.

Nunca debería modificarse automáticamente una cuenta bancaria únicamente porque alguien lo solicita.

Pagos a terceros

Un riesgo adicional aparece cuando un proveedor solicita que el pago sea realizado a un tercero que **no figura como parte del contrato**.

Por ejemplo:

Contrato: Empresa A → Empresa B.

Solicitud de pago: Empresa A → Empresa C.

La situación puede tener una explicación legítima, pero debe ser revisada antes de efectuar el pago.

La organización debería determinar:

- Por qué se solicita el cambio.
- Qué relación existe entre B y C.
- Quién es el propietario de C.
- Si el contrato permite la operación.
- Si existen riesgos de soborno o conflicto de interés.
- Quién debe autorizar la excepción.

Pagos en efectivo

El efectivo puede presentar dificultades adicionales de trazabilidad.

Por ello, una organización puede establecer **límites y restricciones para operaciones en efectivo**, especialmente para determinados tipos de pagos.

Los controles pueden incluir:

- Límites máximos.
- Autorización especial.

- Justificación documental.
- Registro de caja.
- Conciliaciones.
- Revisión periódica.

Cuando resulte apropiado, el uso de **medios de pago trazables** facilita la supervisión de las operaciones.

Pagos urgentes

Las operaciones urgentes pueden representar un desafío para los controles.

Un trabajador puede argumentar:

“Es urgente y debemos pagar hoy.”

La urgencia comercial o operativa no debería significar automáticamente que se eliminen los controles antisoborno.

Cuando sea necesario realizar un pago urgente, la organización puede establecer **procedimientos especiales de autorización**, manteniendo los controles esenciales.

La rapidez no debería convertirse en una justificación para eliminar:

- Verificación.
- Autorización.
- Documentación.
- Registro.
- Trazabilidad.

Fraccionamiento de pagos

El fraccionamiento consiste en dividir una operación en varias transacciones de menor importe. Por ejemplo:

En lugar de una operación de S/ 100 000, podrían registrarse diez pagos de S/ 10 000.

Si los procedimientos internos establecen niveles de autorización diferentes según el importe, el fraccionamiento deliberado podría utilizarse para **evitar un nivel superior de control**.

Por ello, los sistemas de control deberían poder identificar operaciones relacionadas que, en conjunto, representen una transacción de mayor valor.

Pagos de comisiones

Las comisiones deben estar relacionadas con **servicios legítimos y verificables**.

Antes de efectuar una comisión, la organización debería poder determinar:

- Quién la recibe.
- Qué servicio prestó.
- Cuál es la base de cálculo.
- Por qué corresponde ese importe.
- Qué contrato la respalda.
- Quién la aprobó.
- Qué documentación existe.

Las comisiones extraordinariamente elevadas o sin justificación suficiente deben ser objeto de **revisión adicional**.

Honorarios de consultores e intermediarios

Los pagos a consultores, agentes e intermediarios pueden presentar riesgos especiales porque estas personas pueden actuar frente a terceros o funcionarios en nombre de la organización.

La organización debería combinar:

Debida diligencia + contrato + controles de pago + supervisión.

La existencia de un contrato por sí sola no garantiza que el riesgo esté controlado.

También debe existir evidencia razonable de que **el servicio contratado fue realmente prestado y que el pago corresponde a ese servicio**.

Pagos relacionados con funcionarios públicos

Cuando una operación involucra directa o indirectamente a un funcionario público, debe aplicarse especial cuidado. Por ejemplo, debe evitarse que una factura aparentemente legítima pueda utilizarse para canalizar un beneficio personal hacia un funcionario.

La organización debe analizar especialmente:

- Naturaleza del servicio.
- Beneficiario final.
- Intermediarios.
- Importe.
- Momento del pago.
- Decisiones pendientes.
- Relaciones entre las partes.

La ISO 37001:2025 contempla expresamente el soborno relacionado con los sectores público, privado y sin fines de lucro, incluyendo el soborno realizado mediante terceros.

Pagos relacionados con contrataciones públicas

Cuando una organización participa en contrataciones con el Estado, los controles de pago deben integrarse con los procedimientos internos y con las obligaciones legales aplicables.

Los pagos relacionados con:

- Contratos públicos.
- Servicios al Estado.
- Obras.
- Consultorías.
- Subcontrataciones.
- Valorizaciones.
- Adicionales.
- Liquidaciones.

pueden requerir **niveles adecuados de revisión y documentación**.

La organización debe evitar que los pagos sean utilizados para influir indebidamente en funcionarios o para obtener ventajas que no correspondan.

Pagos por servicios inexistentes

Una de las situaciones de mayor riesgo es la utilización de una operación ficticia para justificar una salida de dinero. Por ejemplo:

Una empresa registra:

“Servicios de asesoría administrativa — S/ 80 000”.

Sin embargo:

- No existe informe.
- No existe evidencia del trabajo.
- El proveedor no tiene capacidad aparente.
- La persona que autorizó la contratación tiene una relación personal con el proveedor.

La situación requiere una **revisión inmediata y documentada**.

Registros contables

La aprobación del pago debe estar conectada con un registro contable adecuado.

La información registrada debe reflejar correctamente:

- Importe.
- Fecha.
- Beneficiario.
- Naturaleza del gasto.

- Cuenta contable.
- Documento de respaldo.

Los registros contables no deben utilizarse para ocultar la verdadera naturaleza de una operación. Esto es especialmente importante porque un soborno puede intentar presentarse como un gasto comercial aparentemente legítimo.

Niveles de aprobación

Una matriz de autorización puede establecer diferentes niveles.

Por ejemplo:

Importe de la operación	Nivel de aprobación
Hasta S/ 5 000	Responsable del área
S/ 5 001 – S/ 25 000	Jefatura correspondiente
S/ 25 001 – S/ 100 000	Gerencia
Más de S/ 100 000	Nivel superior definido por la organización

Estos importes son **solo un ejemplo didáctico**. Cada organización debe establecer sus propios límites según su tamaño, estructura y nivel de riesgo. Lo importante es que los límites estén **claramente definidos y sean conocidos por las personas responsables**.

Operaciones de alto riesgo

No todas las operaciones deben recibir exactamente el mismo nivel de revisión. Puede ser razonable aplicar controles adicionales cuando una transacción:

- Tiene un importe elevado.
- Involucra un intermediario.
- Se relaciona con un funcionario público.
- Está vinculada a una contratación pública.
- Se realiza en un país o zona de mayor exposición al soborno.
- Implica una cuenta bancaria de un tercero.
- Se aparta de las condiciones contractuales.
- Presenta señales de alerta.

Este enfoque permite aplicar **controles proporcionales al riesgo**, uno de los principios fundamentales del sistema de gestión antisoborno.

Operaciones excepcionales

Una transacción excepcional no necesariamente es incorrecta. Por ejemplo, puede existir una emergencia operacional que requiera contratar rápidamente un proveedor. Sin embargo, cuando se utiliza una excepción, debe quedar documentado:

qué ocurrió, por qué fue necesaria la excepción, quién la autorizó y qué controles se aplicaron.

Esto permite evitar que el concepto de “emergencia” se utilice repetidamente para **evitar los procedimientos ordinarios**.

Conciliaciones

Las conciliaciones permiten comparar los registros internos con la información bancaria u otras fuentes relevantes. Pueden ayudar a detectar:

- Pagos duplicados.
- Pagos no autorizados.
- Diferencias.
- Operaciones desconocidas.
- Beneficiarios incorrectos.
- Errores.
- Transacciones inusuales.

Por ello, las conciliaciones constituyen un **control detectivo importante**.

Revisión posterior

La aprobación inicial no debería ser necesariamente el único control. Dependiendo del nivel de riesgo, pueden realizarse revisiones posteriores mediante:

- Auditorías.
- Muestreos.
- Análisis de operaciones.
- Revisiones de proveedores.
- Controles internos.
- Conciliaciones.
- Evaluaciones periódicas.

Esto permite comprobar si los controles funcionan **en la práctica y no solamente en los documentos**.

Señales de alerta en pagos y transacciones

Entre las situaciones que pueden requerir una investigación o revisión adicional se encuentran:

- Pago sin contrato o documentación suficiente.
- Facturas con conceptos vagos.
- Pagos a cuentas de terceros.
- Solicitudes de efectivo.
- Cambios inesperados de cuentas bancarias.
- Pagos divididos artificialmente.
- Comisiones desproporcionadas.
- Servicios difíciles de demostrar.
- Pagos urgentes sin explicación.

- Proveedores relacionados con funcionarios.
- Operaciones fuera del procedimiento habitual.
- Solicitudes para evitar controles.

Una señal de alerta no demuestra que exista soborno. Su función es identificar una situación que merece ser analizada.

Caso práctico: factura sin evidencia

Una empresa recibe una factura de S/ 35 000 por “servicios de gestión comercial”. El responsable solicita que se pague inmediatamente.

Al revisar la documentación, Finanzas observa que:

- No existe contrato firmado.
- No existe informe del servicio.
- No está claro qué trabajo se realizó.
- El proveedor fue creado recientemente.

La organización debería **suspender temporalmente la aprobación y solicitar información adicional**. El objetivo no es acusar al proveedor, sino comprobar que la operación sea legítima antes de utilizar los recursos de la organización.

Caso práctico: pago a una cuenta diferente

Un proveedor habitual solicita que el siguiente pago se realice a una cuenta perteneciente a otra empresa. El trabajador responsable podría simplemente modificar los datos bancarios.

Sin embargo, un sistema de control adecuado requiere:

verificar → documentar → autorizar → actualizar → pagar.

Esta secuencia reduce el riesgo de que una modificación fraudulenta o indebida pueda convertirse en un pago real.

Caso práctico: operación fraccionada

Un departamento necesita contratar un servicio por S/ 60 000. El procedimiento interno establece que las operaciones superiores a S/ 50 000 requieren aprobación de la gerencia. El responsable divide artificialmente la contratación en tres órdenes de S/ 20 000.

Aunque cada orden individual esté por debajo del límite, **el conjunto de operaciones corresponde a una única necesidad comercial**.

El sistema de control debe identificar este tipo de situaciones y evitar que el fraccionamiento sea utilizado para eludir las autorizaciones.

Caso práctico: pago urgente

Una empresa necesita realizar una reparación urgente y debe contratar un proveedor inmediatamente. La situación puede justificar un procedimiento extraordinario. Sin embargo, la organización debería conservar evidencia de:

- Motivo de la urgencia.
- Proveedor seleccionado.
- Importe.
- Responsable que autorizó.
- Servicio realizado.
- Pago efectuado.

De esta manera, **la excepción queda documentada y puede ser revisada posteriormente**.

Documentación de las aprobaciones

Las aprobaciones deben dejar evidencia suficiente. Dependiendo de los sistemas utilizados, puede existir:

- Firma.
- Aprobación electrónica.
- Registro en un sistema.
- Correo corporativo autorizado.
- Orden de pago.
- Formulario interno.
- Registro documental.

Lo importante es que pueda demostrarse **quién aprobó, cuándo aprobó y qué operación estaba aprobando**.

Prohibición de aprobar operaciones propias

Cuando sea posible, debe evitarse que una persona pueda **aprobar sus propios gastos o transacciones sin una revisión independiente**. Por ejemplo, una persona que realiza un gasto de representación no debería ser la única responsable de aprobar posteriormente su propio reembolso. La separación de funciones ayuda a reducir este riesgo.

Integración con el sistema antisoborno

La aprobación de pagos no debe funcionar como un procedimiento financiero aislado.

Debe estar conectado con:

Evaluación de riesgos → debida diligencia → contratación → ejecución → aprobación → pago → registro → supervisión.

Esta integración permite que el riesgo antisoborno sea considerado **durante todo el ciclo de una operación**. ISO señala que los controles financieros y no financieros forman parte de los elementos centrales de un sistema de gestión antisoborno junto con la evaluación de riesgos, debida diligencia, capacitación, monitoreo, investigación, auditoría y mejora continua.

Idea clave

La **aprobación de pagos y transacciones** debe garantizar que los recursos de la organización solo sean utilizados cuando exista una **finalidad legítima, documentación suficiente, autorización adecuada y trazabilidad**.

Un sistema eficaz debe procurar que:

Ninguna persona tenga control absoluto sobre toda la operación.

Los pagos estén respaldados por documentación.

Los bienes y servicios puedan ser verificados.

Los proveedores y terceros sean adecuadamente identificados.

Las cuentas bancarias estén verificadas.

Las operaciones excepcionales sean revisadas.

Los pagos de mayor riesgo reciban controles adicionales.

Los registros contables reflejen correctamente la realidad de las operaciones.

Las aprobaciones puedan ser demostradas mediante evidencia.

En definitiva, **aprobar un pago no significa simplemente autorizar una transferencia de dinero**. Significa verificar que la operación sea legítima, que corresponda a una obligación real de la organización y que se hayan aplicado los controles necesarios para reducir el riesgo de soborno.

Este enfoque es coherente con **ISO 37001:2025**, que establece un marco para implementar controles financieros y no financieros de manera razonable y proporcional al riesgo de soborno.

5.3. Canales de denuncia (whistleblowing)

Introducción

Los **canales de denuncia** constituyen un mecanismo fundamental dentro de un Sistema de Gestión Antisoborno, porque permiten que las personas comuniquen **sospechas, preocupaciones o posibles incumplimientos relacionados con el soborno** de manera organizada y segura.

La **ISO 37001:2025** incluye los mecanismos de reporte, seguimiento e investigación entre los elementos de un sistema de gestión antisoborno. La norma está orientada a que las organizaciones puedan **prevenir, detectar y responder al soborno**, aplicando medidas razonables y proporcionales a sus riesgos.

Un canal de denuncia no debe entenderse únicamente como un medio para presentar una acusación. También debe permitir que una persona **plantee una preocupación de buena fe cuando observa una situación que podría representar un riesgo de soborno**.

¿Qué es un canal de denuncia?

Un canal de denuncia es un **medio establecido por la organización para recibir comunicaciones relacionadas con posibles conductas indebidas**.

Puede utilizarse para informar, por ejemplo, sobre:

- Solicitudes de sobornos.
- Ofrecimiento de pagos indebidos.
- Regalos o beneficios sospechosos.
- Pagos no justificados.
- Manipulación de documentos.
- Conflictos de interés no declarados.
- Uso indebido de recursos.
- Operaciones comerciales inusuales.
- Presiones para incumplir controles antisoborno.
- Conductas de terceros relacionadas con la organización.
- Incumplimientos de la política antisoborno.

El canal debe permitir que la organización **reciba, registre, evalúe y gestione adecuadamente las comunicaciones recibidas**.

¿Quién puede utilizar los canales de denuncia?

Los canales no deberían limitarse exclusivamente a los trabajadores. Dependiendo del diseño del sistema y del contexto de la organización, pueden estar disponibles para:

- Trabajadores.
- Directivos.
- Gerentes.
- Contratistas.
- Proveedores.
- Consultores.
- Socios de negocio.
- Clientes.
- Personas que actúan en nombre de la organización.
- Otros terceros relacionados con sus actividades.

Esto resulta especialmente importante porque el soborno puede producirse **directamente o mediante terceros**. ISO 37001:2025 contempla expresamente las relaciones con socios de negocio y diferentes formas de soborno en organizaciones públicas, privadas y sin fines de lucro.

¿Qué debería poder comunicarse?

Un canal de denuncia debe permitir comunicar situaciones que puedan representar **un riesgo real o potencial de soborno**. Por ejemplo, un trabajador podría informar:

“Un proveedor me ha ofrecido un beneficio personal si recomiendo que su empresa sea seleccionada.”

También podría comunicar:

“Me han solicitado registrar un servicio que aparentemente nunca fue realizado.”

O:

“Un tercero relacionado con la empresa está solicitando un pago adicional que no aparece en el contrato.”

En estos casos, la persona **no necesariamente tiene que demostrar que existe un soborno**. Su función inicial consiste en comunicar una situación que considera preocupante para que sea evaluada.

Diferencia entre denuncia y sospecha

Es importante distinguir entre **comunicar una preocupación** y **determinar que se ha cometido una infracción**. Una persona puede observar determinadas circunstancias que le resultan inusuales, pero no disponer de toda la información.

Por ejemplo:

- Un pago elevado.
- Un proveedor desconocido.
- Una solicitud de efectivo.
- Una modificación inusual de un contrato.

Estas circunstancias pueden justificar una comunicación, pero **no demuestran por sí mismas que exista soborno**. La investigación posterior debe determinar qué ocurrió realmente.

Principio de buena fe

Las organizaciones deben fomentar que las personas puedan comunicar sus preocupaciones **de buena fe**, sin exigirles que tengan certeza absoluta sobre los hechos. Una persona puede equivocarse en su interpretación y, aun así, haber actuado correctamente al comunicar una situación que razonablemente consideraba preocupante.

Por ello, es importante crear una cultura en la que los trabajadores entiendan que:

Informar una preocupación no significa acusar automáticamente a una persona de corrupción.

Confidencialidad

Uno de los elementos más importantes de un canal de denuncia es la **protección de la información recibida**. La organización debe establecer mecanismos para controlar quién puede acceder a las comunicaciones y a la documentación relacionada con ellas.

La información debería tratarse de acuerdo con las **obligaciones legales aplicables, las políticas internas y los principios de confidencialidad y protección de datos**. El acceso debe limitarse a las personas que necesitan conocer la información para realizar sus funciones.

Protección de la identidad

Dependiendo del sistema utilizado y de las obligaciones legales aplicables, puede existir la posibilidad de presentar comunicaciones **confidenciales o anónimas**. La confidencialidad significa que la identidad del denunciante es conocida por determinadas personas autorizadas, pero no se divulga innecesariamente.

El anonimato significa que la identidad del denunciante **no es conocida por la organización o por quienes reciben inicialmente la comunicación**. La organización debe determinar el modelo aplicable teniendo en cuenta su legislación, estructura y riesgos.

Protección frente a represalias

Un canal de denuncia será poco efectivo si las personas consideran que informar puede provocarles consecuencias negativas. Por ello, la organización debe establecer medidas para **proteger frente a represalias a las personas que comunican preocupaciones de buena fe**, de acuerdo con las leyes aplicables y las políticas internas.

Las represalias pueden adoptar diferentes formas, por ejemplo:

- Amenazas.
- Intimidación.
- Hostigamiento.
- Despido injustificado.
- Reducción injustificada de responsabilidades.
- Cambios perjudiciales en las condiciones laborales.
- Discriminación.
- Exclusión deliberada.
- Otras acciones adversas relacionadas con la comunicación realizada.

La existencia de un canal no es suficiente. **Las personas deben tener confianza en que podrán utilizarlo sin sufrir represalias indebidas.**

Canales disponibles

Una organización puede establecer diferentes mecanismos para recibir comunicaciones.

Entre ellos pueden encontrarse:

- Correo electrónico específico.
- Formulario electrónico.
- Plataforma digital.
- Línea telefónica.
- Canal presencial.
- Comunicación escrita.
- Sistema interno de reportes.
- Canal administrado por un tercero independiente.

No existe un único formato que sea adecuado para todas las organizaciones. La selección debe considerar **el tamaño, estructura, recursos, riesgos y características de la organización**.

Canal interno y canal externo

Los canales pueden ser administrados directamente por la organización o mediante un **proveedor externo especializado**. Por ejemplo, una empresa puede contratar una plataforma independiente para recibir comunicaciones y administrar el acceso a los casos.

Esto puede resultar útil cuando la organización desea aumentar la percepción de **independencia y confidencialidad**. Sin embargo, contratar un tercero no elimina la responsabilidad de la organización de garantizar que las comunicaciones sean **adecuadamente evaluadas y gestionadas**.

Accesibilidad del canal

Un canal de denuncia debe ser **fácil de encontrar y utilizar**. Los trabajadores y socios de negocio deberían saber:

- Que existe.
- Para qué sirve.
- Cómo utilizarlo.
- Qué tipo de situaciones pueden comunicarse.
- Quién recibe la información.
- Qué medidas de confidencialidad existen.
- Qué protección está disponible.
- Qué ocurre después de presentar una comunicación.

Un canal que existe formalmente pero que nadie conoce **no cumple adecuadamente su función preventiva y detectiva**.

Comunicación del canal

La existencia del canal debe comunicarse de forma periódica. Puede incluirse información en:

- Manuales internos.
- Política antisoborno.

- Código de conducta.
- Contratos.
- Material de capacitación.
- Intranet.
- Página web.
- Procesos de incorporación de trabajadores.
- Comunicación dirigida a proveedores y socios de negocio.

La ISO 37001 considera relevante la comunicación de la política antisoborno tanto al personal como a los socios de negocio.

Registro de las comunicaciones

Las comunicaciones recibidas deben registrarse de manera controlada. El registro puede incluir:

- Fecha de recepción.
- Canal utilizado.
- Naturaleza de la preocupación.
- Área relacionada.
- Nivel inicial de riesgo.
- Responsable de evaluación.
- Medidas adoptadas.
- Estado del caso.
- Resultado de la investigación.
- Acciones posteriores.

El registro debe proteger adecuadamente la información sensible.

Evaluación inicial

No todas las comunicaciones requieren exactamente el mismo tratamiento. Una primera evaluación puede determinar:

¿La comunicación está relacionada con el ámbito antisoborno?

¿Existe información suficiente para realizar una evaluación inicial?

¿Existe un riesgo inmediato?

¿Hay posibles conflictos de interés?

¿Quién debe gestionar el caso?

¿Es necesario preservar documentación o evidencia?

Esta evaluación permite determinar **qué respuesta resulta proporcional a la naturaleza y gravedad de la situación**.

Clasificación del riesgo

Las comunicaciones pueden clasificarse según su nivel de riesgo. Por ejemplo:

Riesgo bajo: preocupación administrativa sin indicios relevantes de soborno.

Riesgo medio: existen circunstancias inusuales que requieren revisión.

Riesgo alto: existen indicios concretos de un posible pago indebido, conflicto de interés grave o participación de funcionarios públicos.

Esta clasificación es únicamente un ejemplo. Cada organización debe establecer sus propios criterios.

Independencia en la gestión

Las personas encargadas de recibir o investigar denuncias deben actuar con **objetividad e independencia suficientes**. Un caso no debería ser gestionado por una persona que tenga un interés personal en el resultado.

Por ejemplo, si la comunicación involucra al gerente de un área, no sería adecuado que el propio gerente controlara unilateralmente la investigación. La organización debe establecer mecanismos para **gestionar los conflictos de interés en la investigación de comunicaciones**.

Investigación

Cuando una comunicación presenta indicios razonables de una conducta indebida, puede ser necesario iniciar una investigación.

La investigación debe buscar determinar:

- Qué ocurrió.
- Cuándo ocurrió.
- Quiénes participaron.
- Qué operaciones estuvieron involucradas.
- Qué documentos existen.
- Qué controles fueron aplicados.
- Si hubo incumplimiento.
- Qué riesgos adicionales existen.

La investigación debe realizarse de manera **objetiva, documentada y proporcional al caso**.

Preservación de evidencias

Cuando existe una sospecha relevante, puede ser necesario preservar información relacionada con el caso. Dependiendo de la situación, puede incluir:

- Contratos.
- Facturas.
- Correos electrónicos.
- Registros contables.
- Órdenes de compra.
- Comunicaciones internas.
- Registros de aprobación.
- Documentos de proveedores.
- Información de transacciones.

La organización debe actuar respetando las **leyes aplicables, los derechos de las personas involucradas y las reglas internas de gestión de información**.

No prejuzgar

Una investigación no debe comenzar con la conclusión de que una persona es culpable. El objetivo consiste en **establecer los hechos y evaluar las evidencias disponibles**.

Por ejemplo, recibir una denuncia contra un trabajador no significa que la organización deba sancionarlo inmediatamente. Primero debe determinarse:

qué se comunicó → qué evidencia existe → qué ocurrió realmente → qué normas o controles podrían haberse incumplido.

Comunicación de resultados

Una vez concluida una investigación, la organización puede determinar las acciones correspondientes de acuerdo con sus procedimientos y obligaciones legales.

Estas pueden incluir:

- Cierre del caso.
- Medidas correctivas.
- Mejoras en los controles.
- Capacitación adicional.
- Medidas disciplinarias cuando correspondan.
- Revisión de un proveedor.
- Modificación de procedimientos.
- Comunicación a las autoridades competentes cuando exista obligación legal o corresponda.

No todas las comunicaciones necesariamente terminan en una sanción.

Confidencialidad durante la investigación

La información relacionada con una investigación debe manejarse cuidadosamente. La organización debe evitar divulgar innecesariamente:

- Identidad del denunciante.
- Identidad de la persona investigada.

- Documentos sensibles.
- Información financiera.
- Evidencias.
- Conclusiones preliminares.

La confidencialidad ayuda a proteger **la integridad de la investigación y los derechos de las personas involucradas**.

Relación con la función de cumplimiento

Los canales de denuncia deben estar integrados con la **función de cumplimiento antisoborno**. La función de cumplimiento puede participar, según la estructura de la organización, en:

- Recepción.
- Evaluación.
- Coordinación.
- Investigación.
- Seguimiento.
- Reporte.
- Recomendación de acciones correctivas.

Sin embargo, las responsabilidades concretas deben definirse de acuerdo con la estructura y el sistema de gestión de cada organización.

Relación con la alta dirección

La alta dirección debe demostrar que las comunicaciones relacionadas con posibles actos de soborno **son tomadas en serio**. Esto implica proporcionar los recursos necesarios y evitar que la existencia del canal sea únicamente una formalidad documental.

Una cultura antisoborno efectiva requiere que los trabajadores perciban que:

las denuncias se reciben, se analizan y se gestionan adecuadamente.

Denuncias falsas

La protección de los denunciantes no significa que cualquier comunicación falsa realizada deliberadamente deba quedar sin consecuencias.

La organización puede establecer medidas frente a **acusaciones realizadas deliberadamente con información falsa y con intención de perjudicar a otra persona**, respetando siempre las normas aplicables y los procedimientos internos.

Es importante distinguir entre:

una denuncia equivocada realizada de buena fe

y

una acusación deliberadamente falsa realizada con mala intención.

No deben tratarse de la misma manera.

Relación con ISO 37002

La **ISO 37002:2021** es una norma específica sobre sistemas de gestión de canales de denuncia (Whistleblowing management systems — Guidelines). A diferencia de ISO 37001, que se centra específicamente en la gestión antisoborno, ISO 37002 proporciona orientación más amplia para establecer, implementar, mantener y mejorar un sistema de gestión de denuncias. Ambas normas pueden utilizarse de manera complementaria.

Caso práctico: oferta de un soborno

Un trabajador participa en una negociación con un proveedor. Durante una reunión, el representante del proveedor le ofrece un beneficio personal a cambio de favorecer la adjudicación del contrato.

El trabajador decide utilizar el canal de denuncia de la organización. El procedimiento debería permitir:

Comunicar la situación → registrar la comunicación → evaluar el riesgo → proteger la información → investigar → determinar acciones → mejorar los controles cuando corresponda.

El trabajador no necesita realizar una investigación por su cuenta ni enfrentarse personalmente al proveedor.

Caso práctico: solicitud de un pago

Un empleado recibe una solicitud para realizar un pago adicional que no figura en el contrato.

La persona responsable le indica que el pago es necesario para “agilizar” una autorización. El empleado considera que puede tratarse de un pago indebido.

En este caso, el canal permite **comunicar la preocupación antes de que el pago sea realizado**. Este ejemplo demuestra que los canales de denuncia también cumplen una función **preventiva**, no solamente reactiva.

Caso práctico: proveedor sospechoso

Una organización recibe una comunicación indicando que un proveedor seleccionado mantiene una relación personal con una persona que participa en la decisión de contratación. La comunicación no demuestra que haya existido soborno.

Sin embargo, puede justificar:

- Revisión del conflicto de interés.

- Revisión de la debida diligencia.
- Evaluación del proceso de selección.
- Análisis de las condiciones contractuales.
- Aplicación de medidas adicionales si corresponde.

El canal permite que una señal de alerta llegue a las personas responsables antes de que el riesgo se materialice.

Indicadores de un canal eficaz

Un canal de denuncia bien gestionado debería permitir demostrar que:

Las personas conocen su existencia.

El canal es accesible.

Las comunicaciones son registradas.

La información se mantiene protegida.

Los conflictos de interés son gestionados.

Las comunicaciones se evalúan de manera objetiva.

Los casos se investigan cuando corresponde.

Las personas están protegidas frente a represalias indebidas.

Las acciones adoptadas quedan documentadas.

Las lecciones aprendidas pueden utilizarse para mejorar los controles.

Mejora continua a partir de las denuncias

Las denuncias no solo sirven para identificar posibles incumplimientos individuales. También pueden revelar **debilidades estructurales del sistema**.

Por ejemplo, si varias comunicaciones señalan problemas relacionados con proveedores, la organización podría descubrir que:

- La debida diligencia es insuficiente.
- Los criterios de selección no están claramente definidos.
- Los controles de contratación son débiles.
- Los trabajadores no conocen adecuadamente los procedimientos.

En este caso, la respuesta adecuada no debería limitarse al caso individual. La organización debería analizar **qué cambios pueden evitar que situaciones similares vuelvan a producirse**.

Idea clave

Los **canales de denuncia son una herramienta esencial para detectar y gestionar riesgos de soborno** porque permiten que la información llegue a la organización desde las personas que pueden encontrarse directamente expuestas a situaciones de riesgo.

Un sistema eficaz debe procurar que:

Las personas sepan cómo comunicar una preocupación.

El canal sea accesible y confiable.

Las comunicaciones puedan realizarse de forma confidencial y, cuando corresponda, anónima.

Las personas que actúan de buena fe estén protegidas frente a represalias indebidas.

Las comunicaciones sean evaluadas objetivamente.

Las investigaciones sean proporcionales y documentadas.

Los conflictos de interés sean gestionados.

Las evidencias sean protegidas adecuadamente.

Los resultados permitan adoptar acciones correctivas y preventivas.

La información obtenida contribuya a la mejora continua del Sistema de Gestión Antisoborno.

En definitiva, **un canal de denuncia no es simplemente un buzón para recibir quejas**. Es un componente del sistema de control que permite a la organización **escuchar, detectar, investigar y responder ante posibles situaciones de soborno**, fortaleciendo una cultura de integridad y transparencia. ISO 37001:2025 incorpora precisamente el reporte, seguimiento, investigación, acciones correctivas y mejora continua dentro del enfoque integral del sistema de gestión antisoborno.

5.4. Investigación de incidentes

Introducción

La **investigación de incidentes relacionados con el soborno** es una actividad esencial dentro de un Sistema de Gestión Antisoborno. Su finalidad es determinar, de manera objetiva y documentada, **qué ocurrió, cómo ocurrió, quiénes estuvieron involucrados, qué controles pudieron haber fallado y qué medidas deben adoptarse**.

La **ISO 37001:2025**, actualmente vigente, establece un enfoque orientado a **prevenir, detectar y responder al soborno**. Dentro de este enfoque se incluyen los mecanismos de reporte, seguimiento, investigación, auditoría, acciones correctivas y mejora continua.

Una investigación no debe entenderse únicamente como una búsqueda de responsables. También debe servir para **identificar las causas del incidente y fortalecer el sistema para evitar que una situación similar vuelva a producirse**.

¿Qué es un incidente antisoborno?

Un incidente antisoborno es una situación en la que existe una **sospecha, indicio, incumplimiento o evidencia relacionada con una posible conducta de soborno** o con una vulneración de los controles establecidos para prevenirlo.

Puede estar relacionado, por ejemplo, con:

- Una solicitud de pago indebido.
- Un ofrecimiento de dinero o beneficio personal.
- Un regalo utilizado para influir en una decisión.
- Una comisión injustificada.
- Un pago a un tercero no autorizado.
- Una factura por servicios inexistentes.
- Manipulación de registros financieros.
- Ocultamiento de información.
- Incumplimiento de la política antisoborno.
- Incumplimiento de un procedimiento de control.
- Conductas de un socio de negocio.
- Intentos de evitar los controles establecidos.

No todo incidente constituye necesariamente un soborno. Una señal de alerta o una denuncia debe ser evaluada antes de llegar a una conclusión.

Diferencia entre alerta, incidente y soborno confirmado

Es importante utilizar correctamente estos conceptos. Una **señal de alerta** es una circunstancia que puede indicar la existencia de un riesgo. Un **incidente** es una situación que requiere evaluación o investigación debido a un posible incumplimiento o conducta irregular. Un **soborno confirmado** es una conclusión basada en evidencias y en el proceso de evaluación correspondiente.

Por ejemplo, recibir una denuncia de que un proveedor ofreció dinero a un trabajador **no significa automáticamente que el soborno esté demostrado**. Significa que existe información suficiente para considerar una evaluación o investigación.

¿Cuándo debe investigarse un incidente?

La organización debe establecer criterios para determinar **cuándo una comunicación o situación requiere una investigación formal**.

Algunos factores que pueden justificar una investigación son:

- Existencia de evidencias iniciales.
- Posible incumplimiento de la política antisoborno.
- Participación de un trabajador.

- Participación de un socio de negocio.
- Posible participación de un funcionario público.
- Pagos o transacciones sospechosas.
- Manipulación de documentos.
- Reincidencia.
- Riesgo financiero significativo.
- Riesgo reputacional.
- Posible incumplimiento legal.

La respuesta debe ser **proporcional a la naturaleza y gravedad del caso**.

Principios de una investigación

Una investigación antisoborno debe desarrollarse siguiendo principios que permitan preservar su credibilidad. Entre los más importantes se encuentran:

Objetividad: las conclusiones deben basarse en hechos y evidencias.

Imparcialidad: las personas involucradas deben ser evaluadas sin prejuicios.

Confidencialidad: la información debe compartirse únicamente con quienes necesitan conocerla.

Independencia: quienes investigan no deben tener conflictos de interés con el caso.

Proporcionalidad: el nivel de investigación debe corresponder a la gravedad y al riesgo.

Documentación: las principales actuaciones y decisiones deben quedar registradas.

Recepción del caso

Una investigación puede comenzar a partir de diferentes fuentes.

Por ejemplo:

- Canal de denuncia.
- Auditoría interna.
- Revisión financiera.
- Control interno.
- Supervisión de proveedores.
- Reporte de un trabajador.
- Revisión de una transacción.
- Información recibida de un socio de negocio.
- Hallazgo de la función de cumplimiento.
- Información procedente de una autoridad competente.

La organización debe contar con un procedimiento que permita **recibir, registrar y evaluar estas situaciones de manera ordenada**.

Evaluación inicial

Antes de iniciar una investigación completa, puede realizarse una **evaluación inicial del caso**.

Esta etapa permite determinar:

- Qué información se ha recibido.
- Qué hechos están siendo comunicados.
- Qué personas o áreas podrían estar involucradas.
- Qué riesgos existen.
- Si existe información suficiente para continuar.
- Si existe un posible conflicto de interés.
- Qué medidas inmediatas pueden ser necesarias.

La evaluación inicial no debe utilizarse para descartar automáticamente una denuncia simplemente porque todavía no existen pruebas completas.

Preservación de información

Cuando existe una sospecha razonable, puede ser necesario **preservar información relevante antes de iniciar determinadas actuaciones**.

Dependiendo del caso, puede incluir:

- Contratos.
- Facturas.
- Órdenes de compra.
- Registros contables.
- Correos electrónicos.
- Comunicaciones corporativas.
- Informes.
- Registros de aprobación.
- Documentación de proveedores.
- Registros de pagos.
- Documentación relacionada con la operación.

La preservación debe realizarse respetando las **leyes aplicables, las políticas internas y las obligaciones de protección de datos y confidencialidad**.

Planificación de la investigación

Una investigación debe organizarse antes de realizar las principales actuaciones.

El plan puede determinar:

Qué hechos deben aclararse.

Qué documentación debe revisarse.

Qué personas deben ser entrevistadas.

Quién dirigirá la investigación.

Qué recursos serán necesarios.

Qué riesgos deben gestionarse.

Qué plazos son razonables.

No todos los casos requieren una investigación compleja. Un incidente de bajo riesgo puede requerir una revisión limitada, mientras que un posible soborno de alto valor puede necesitar una investigación mucho más profunda.

Independencia del investigador

Las personas responsables de investigar deben contar con un nivel adecuado de **independencia y objetividad**. Por ejemplo, si una denuncia involucra al responsable directo del investigador, puede existir un conflicto de interés.

En estos casos, la organización debe establecer mecanismos para:

- Designar a otra persona.
- Elevar el caso a un nivel superior.
- Solicitar apoyo de la función de cumplimiento.
- Utilizar especialistas externos cuando sea necesario.

Una investigación pierde credibilidad cuando la persona que podría verse afectada controla el resultado de la investigación.

Función de cumplimiento

La **función de cumplimiento antisoborno** puede desempeñar un papel importante en la investigación, dependiendo de la estructura y responsabilidades definidas por la organización.

Puede participar en:

- Evaluación inicial.
- Coordinación.
- Supervisión.
- Asesoramiento.
- Seguimiento.
- Comunicación de resultados.
- Recomendación de medidas correctivas.

La ISO 37001 contempla la existencia de una función responsable de supervisar el sistema antisoborno y también incluye la investigación y el seguimiento como elementos del sistema.

Recopilación de evidencias

La investigación debe buscar **evidencias relevantes y verificables**. Estas pueden incluir:

- Documentos contractuales.
- Registros financieros.
- Facturas.
- Comprobantes de pago.
- Correos corporativos.
- Mensajes relacionados con la operación.
- Registros de aprobación.
- Informes.
- Documentos de proveedores.
- Información sobre relaciones entre las partes.
- Registros de reuniones.

La evidencia debe analizarse considerando **su origen, autenticidad, relevancia y relación con los hechos investigados**.

Entrevistas

Las entrevistas pueden ser necesarias para comprender cómo ocurrieron los hechos.

Dependiendo del caso, pueden entrevistarse:

- Persona que realizó la denuncia.
- Trabajadores involucrados.
- Responsables de la operación.
- Proveedores.
- Testigos.
- Responsables de aprobación.
- Personas que participaron en la contratación.

Las entrevistas deben realizarse de forma **profesional, objetiva y respetuosa**, evitando presionar a las personas para obtener una determinada respuesta.

Preguntas durante una investigación

Las preguntas deben orientarse a establecer hechos. Por ejemplo:

¿Qué ocurrió?

¿Cuándo ocurrió?

¿Quiénes participaron?

¿Quién tomó la decisión?

¿Qué documentación existe?

¿Quién autorizó la operación?

¿Qué comunicación existió entre las partes?

¿Se produjo algún pago o beneficio?

¿Existía una relación previa entre las personas involucradas?

¿Se siguieron los procedimientos internos?

Estas preguntas ayudan a construir una **secuencia objetiva de los acontecimientos**.

Análisis de transacciones

Cuando el incidente está relacionado con dinero, debe analizarse la operación financiera.

Puede revisarse:

- Importe.
- Fecha.
- Beneficiario.
- Cuenta bancaria.
- Concepto.
- Autorizaciones.
- Factura.
- Contrato.
- Relación con otras operaciones.

También puede analizarse si existen **operaciones relacionadas que, individualmente, parecen normales pero que en conjunto presentan un patrón inusual**.

Análisis de terceros

Cuando el incidente involucra a un proveedor, agente, consultor o socio de negocio, puede ser necesario revisar la información disponible sobre dicho tercero.

La investigación puede considerar:

- Identidad.
- Propietarios.
- Representantes.
- Relación contractual.
- Servicios prestados.
- Historial de operaciones.
- Pagos realizados.
- Personas relacionadas.
- Posibles conflictos de interés.

Esto permite determinar si el incidente es **aislado o forma parte de un riesgo más amplio relacionado con el tercero**.

Relación con funcionarios públicos

Los casos que puedan involucrar a **funcionarios públicos** requieren especial atención debido a las posibles consecuencias legales y reputacionales.

Por ejemplo, debe investigarse cuidadosamente una situación en la que:

- Un intermediario solicita dinero para “agilizar” un trámite.
- Un trabajador ofrece un beneficio a un funcionario.
- Un proveedor afirma tener influencia sobre una decisión pública.
- Se realiza un pago no previsto durante una contratación pública.

La organización debe considerar también las **obligaciones legales aplicables y, cuando corresponda, la necesidad de comunicar determinados hechos a las autoridades competentes**.

No prejuzgar a las personas

Una investigación debe partir de una posición de **objetividad**. La existencia de una denuncia no significa que la persona denunciada sea culpable.

Debe distinguirse entre:

una acusación,
una sospecha,
una evidencia,
un hecho comprobado
y **una conclusión de la investigación**.

Esta distinción es fundamental para proteger la integridad del proceso.

Confidencialidad

La información de una investigación debe mantenerse bajo **estrictos controles de acceso**. No es apropiado compartir indiscriminadamente:

- Nombre del denunciante.
- Nombre de la persona investigada.
- Evidencias.
- Información financiera.
- Declaraciones.
- Conclusiones preliminares.

La divulgación innecesaria puede perjudicar tanto a la investigación como a las personas involucradas.

Protección frente a represalias

Las personas que comuniquen una preocupación de buena fe deben contar con las **protecciones establecidas por la organización y por la legislación aplicable**. Una persona no debería ser castigada simplemente por haber comunicado honestamente una preocupación que posteriormente no pudo confirmarse.

Esto es especialmente importante para construir una cultura en la que los trabajadores estén dispuestos a **reportar situaciones potencialmente riesgosas**.

Medidas inmediatas

En determinados casos puede ser necesario adoptar medidas antes de terminar la investigación.

Por ejemplo:

- Suspender temporalmente un pago.
- Limitar el acceso a determinados documentos.
- Separar determinadas funciones.
- Reforzar la supervisión de una operación.
- Suspender temporalmente una relación comercial cuando corresponda.
- Preservar información relevante.

Estas medidas deben ser **proporcionales y adecuadamente justificadas**.

Determinación de los hechos

El objetivo principal de la investigación es establecer, en la medida razonablemente posible: **qué ocurrió, cuándo ocurrió, cómo ocurrió, quién participó y qué controles estuvieron involucrados.**

También debe determinarse si existe evidencia suficiente para concluir que:

- No existió incumplimiento.
- Existió una debilidad de control.
- Existió un incumplimiento interno.
- Existió una conducta indebida.
- Existió un posible acto de soborno.
- Se requiere una investigación o actuación adicional.

Causas del incidente

Una investigación eficaz no debería detenerse en identificar **quién realizó una acción incorrecta**. También debe preguntarse:

¿Por qué pudo ocurrir?

Puede descubrirse, por ejemplo, que:

- El procedimiento era ambiguo.
- No existía separación de funciones.
- El trabajador no había recibido capacitación.
- El proveedor no había sido sometido a debida diligencia.
- El nivel de autorización era insuficiente.
- No existía supervisión.
- El canal de denuncia no era conocido.
- Los controles financieros eran débiles.

Esto permite pasar de una respuesta exclusivamente disciplinaria a una **mejora real del sistema de gestión**.

Análisis de causa raíz

El análisis de causa raíz busca identificar los factores que permitieron que el incidente ocurriera. Por ejemplo:

Incidente: pago indebido a un intermediario.

Causa inmediata: se realizó un pago sin documentación suficiente.

Debilidad de control: no existía una segunda aprobación.

Causa organizacional: el procedimiento financiero permitía excepciones sin revisión independiente.

Medida correctiva: modificar el procedimiento y establecer un control adicional para operaciones de mayor riesgo.

Este enfoque permite **evitar que la organización se limite a solucionar únicamente el caso individual**.

Acciones correctivas

Cuando se identifica una no conformidad, la ISO 37001:2025 establece que la organización debe reaccionar ante ella, controlar y corregirla cuando corresponda, tratar sus consecuencias y evaluar la necesidad de acciones destinadas a eliminar las causas para evitar que vuelva a ocurrir. También debe revisar la eficacia de las acciones correctivas y modificar el sistema cuando sea necesario.

Las acciones correctivas pueden incluir:

- Modificación de procedimientos.
- Nuevos controles financieros.
- Revisión de proveedores.
- Capacitación.
- Reorganización de funciones.
- Refuerzo de autorizaciones.
- Actualización de la política antisoborno.
- Mejora del canal de denuncia.

- Mayor supervisión.

Diferencia entre corrección y acción correctiva

Es importante distinguir ambos conceptos.

La **corrección** busca solucionar el problema concreto que ya ocurrió.

La **acción correctiva** busca eliminar o reducir la causa que permitió que el problema ocurriera, con el objetivo de evitar su repetición.

Por ejemplo:

Corrección: cancelar un pago indebido.

Acción correctiva: modificar el procedimiento de aprobación para evitar que un pago similar pueda aprobarse nuevamente sin controles suficientes.

Evaluación de eficacia

Una acción correctiva no debe considerarse terminada simplemente porque fue implementada.

Debe evaluarse si **realmente funcionó**.

Por ejemplo, si se establece una segunda aprobación para pagos de alto riesgo, posteriormente puede revisarse si:

- La aprobación realmente se está realizando.
- Las personas conocen el nuevo procedimiento.
- Los pagos se encuentran correctamente documentados.
- Las excepciones están justificadas.
- El riesgo disminuyó.

La ISO 37001:2025 requiere revisar la **eficacia de las acciones correctivas** adoptadas.

Documentación de la investigación

La organización debe conservar información documentada suficiente para demostrar cómo fue gestionado el incidente.

Dependiendo del caso, puede incluir:

- Comunicación inicial.
- Evaluación del caso.
- Plan de investigación.
- Evidencias.
- Entrevistas.
- Análisis.
- Conclusiones.

- Decisiones adoptadas.
- Acciones correctivas.
- Seguimiento.

La documentación debe gestionarse de acuerdo con las **reglas internas y obligaciones legales aplicables**.

Informe final

Una investigación formal puede finalizar con un **informe de investigación**. El informe puede contener:

Antecedentes del caso.

Alcance de la investigación.

Hechos analizados.

Evidencias revisadas.

Personas o áreas involucradas.

Controles relacionados.

Hallazgos.

Conclusiones.

Acciones recomendadas.

Medidas correctivas y de seguimiento.

El nivel de detalle debe ser **proporcional a la gravedad y complejidad del caso**.

Seguimiento

La investigación no termina necesariamente cuando se emite el informe. Debe verificarse que las acciones acordadas sean implementadas.

Por ejemplo:

Se identificó una debilidad → se estableció una acción → se asignó un responsable → se estableció un plazo → se verificó la implementación → se evaluó su eficacia.

Este seguimiento conecta directamente la investigación con la **mejora continua del Sistema de Gestión Antisoborno**.

Aprendizaje organizacional

Cada incidente puede proporcionar información valiosa para mejorar el sistema.

La organización puede preguntarse:

¿Qué aprendimos?

¿Qué control falló?

¿El riesgo estaba correctamente evaluado?

¿La capacitación fue suficiente?

¿La política era clara?

¿La debida diligencia fue adecuada?

¿El canal de denuncia funcionó correctamente?

¿Necesitamos modificar algún procedimiento?

De esta manera, una investigación puede convertirse en una **fuente de aprendizaje y prevención**.

Caso práctico: pago indebido

Un trabajador comunica que un proveedor le ofreció S/ 10 000 para favorecer su selección en un proceso de contratación. La organización registra la comunicación y realiza una evaluación inicial.

Posteriormente:

Se preserva la documentación del proceso.

Se revisan las comunicaciones entre las partes.

Se analizan las condiciones de contratación.

Se revisan las aprobaciones.

Se entrevista a las personas relevantes.

Se analiza al proveedor.

Se determina qué ocurrió.

Si se confirma una conducta indebida, la organización deberá determinar las medidas correspondientes y analizar **qué controles permitieron que la situación ocurriera**.

Caso práctico: factura ficticia

El área financiera detecta una factura por S/ 70 000 correspondiente a un supuesto servicio de consultoría.

Durante la revisión se descubre que:

- No existe evidencia suficiente del servicio.
- La factura fue aprobada rápidamente.
- El proveedor tiene relación con un trabajador.
- El procedimiento de aprobación fue omitido.

La investigación debería analizar no solamente el pago, sino también **la relación entre el trabajador y el proveedor, la contratación, las autorizaciones y las posibles deficiencias del sistema de control**.

Caso práctico: incumplimiento sin soborno

Un trabajador realiza un pago sin obtener una autorización obligatoria. La investigación determina que **no existió soborno**, pero sí un incumplimiento del procedimiento financiero.

En este caso, la organización puede necesitar adoptar una acción correctiva aunque no se haya producido un acto de soborno. Esto demuestra que el Sistema de Gestión Antisoborno también debe gestionar **las debilidades que podrían facilitar futuros incidentes**.

Indicadores de una investigación adecuada

Una investigación correctamente gestionada debería permitir demostrar que:

El caso fue registrado.

Se evaluó su nivel de riesgo.

Se identificaron las personas responsables de gestionarlo.

Se protegió la información relevante.

Se evitaron conflictos de interés.

Se recopilaron evidencias.

Se analizaron los hechos objetivamente.

Se documentaron las conclusiones.

Se determinaron las acciones necesarias.

Se verificó el cumplimiento de las acciones correctivas.

Se evaluó la eficacia de las medidas adoptadas.

Investigación y mejora continua

La investigación de incidentes está directamente relacionada con la **mejora continua**.

La ISO 37001:2025 establece que la organización debe mejorar continuamente la **idoneidad, adecuación y eficacia** de su Sistema de Gestión Antisoborno.

Por ello, un incidente debe analizarse no solo desde la perspectiva de:

"¿Quién hizo algo incorrecto?"

sino también desde:

"¿Qué podemos mejorar para reducir la posibilidad de que vuelva a ocurrir?"

Esta segunda pregunta es fundamental para construir un sistema antisoborno realmente eficaz.

Idea clave

La **investigación de incidentes** permite transformar una sospecha, denuncia o señal de alerta en un proceso estructurado de **análisis, determinación de hechos, corrección y aprendizaje organizacional**.

Una organización debe procurar que:

Los incidentes sean recibidos y evaluados oportunamente.

Las investigaciones sean objetivas e independientes.

Las personas involucradas sean tratadas de manera imparcial.

La información sea protegida.

Las evidencias sean adecuadamente conservadas.

Las conclusiones se basen en hechos y evidencias.

Las causas de los incidentes sean analizadas.

Las acciones correctivas sean proporcionales.

La eficacia de las acciones sea verificada.

Las lecciones aprendidas se incorporen al Sistema de Gestión Antisoborno.

En definitiva, **investigar un incidente no significa únicamente determinar si alguien cometió una conducta indebida**. Significa comprender qué ocurrió, responder adecuadamente y utilizar la experiencia obtenida para **fortalecer los controles, reducir los riesgos y mejorar continuamente el sistema antisoborno**. Este enfoque coincide con la estructura actual de **ISO 37001:2025**, que integra investigación, acciones correctivas y mejora continua dentro del funcionamiento del sistema de gestión.

6. Auditoría, Mejora Continua y Certificación

6.1. Auditoría interna

Introducción

La **auditoría interna** es una herramienta fundamental para evaluar si el Sistema de Gestión Antisoborno funciona realmente en la práctica. No se trata únicamente de comprobar si existen políticas y procedimientos escritos, sino de verificar si estos **han sido implementados, se aplican correctamente y son eficaces para gestionar los riesgos de soborno**.

La versión actualmente vigente de la norma es **ISO 37001:2025**, publicada en febrero de 2025, que sustituyó a ISO 37001:2016. La norma establece requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión Antisoborno.

Dentro de esta estructura, la **cláusula 9.2** está dedicada específicamente a la auditoría interna.

¿Qué es una auditoría interna?

Una auditoría interna es un proceso **sistemático, independiente y documentado** que permite obtener evidencias y evaluarlas objetivamente para determinar si el sistema cumple determinados criterios.

En el contexto de ISO 37001, la auditoría interna permite comprobar principalmente:

Si el Sistema de Gestión Antisoborno cumple los requisitos establecidos por la propia organización.

Si cumple los requisitos aplicables de ISO 37001.

Si el sistema está correctamente implementado.

Si el sistema se mantiene de manera eficaz.

Por tanto, una auditoría no consiste simplemente en preguntar si existe una política antisoborno. Debe determinarse **si esa política se aplica realmente y si los controles establecidos funcionan**.

Objetivo de la auditoría interna

El objetivo principal es proporcionar información fiable sobre el funcionamiento del Sistema de Gestión Antisoborno.

Una auditoría puede ayudar a identificar:

- Incumplimientos de requisitos.
- Debilidades de controles.
- Procedimientos que no se aplican correctamente.
- Riesgos que no han sido adecuadamente gestionados.
- Deficiencias en la documentación.
- Problemas relacionados con socios de negocio.
- Incumplimientos de la política antisoborno.
- Oportunidades de mejora.

La auditoría también puede confirmar que determinados controles **están funcionando adecuadamente**.

La auditoría no es una búsqueda de culpables

Una auditoría interna debe diferenciarse de una investigación disciplinaria. La auditoría busca determinar **si los procesos y controles cumplen los requisitos establecidos y funcionan eficazmente**.

Por ejemplo, si se detecta que varias compras fueron aprobadas sin la documentación requerida, el objetivo de la auditoría no debería limitarse a identificar al trabajador que cometió el error.

También debe analizarse:

¿El procedimiento era claro?

¿El trabajador conocía el procedimiento?

¿Existía supervisión?

¿El sistema permitía aprobar la operación sin documentación?

¿El control estaba correctamente diseñado?

¿El problema era aislado o se repetía en otras operaciones?

Este enfoque permite identificar **debilidades sistémicas**.

Auditorías a intervalos planificados

ISO 37001:2025 establece que la organización debe realizar **auditorías internas a intervalos planificados**. Estas auditorías deben proporcionar información sobre la conformidad y la eficacia del Sistema de Gestión Antisoborno. Esto significa que la organización debe establecer una planificación.

No es suficiente realizar una auditoría únicamente cuando:

- Se aproxima una certificación.
- Se produce un incidente grave.
- Un cliente solicita evidencia.
- Un auditor externo la exige.

La auditoría debe formar parte del **funcionamiento normal del sistema de gestión**.

Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener un **programa de auditoría interna**.

Este programa debe considerar aspectos como:

- Frecuencia de las auditorías.
- Métodos utilizados.
- Responsabilidades.
- Planificación.
- Elaboración de informes.
- Importancia de los procesos.
- Resultados de auditorías anteriores.

La norma establece además que los resultados de las auditorías deben comunicarse a los responsables pertinentes, a la **función antisoborno**, a la **alta dirección** y, cuando corresponda, al órgano de gobierno.

Auditoría basada en riesgos

Las auditorías deben considerar la **importancia y el nivel de riesgo de los procesos**. No todas las áreas de una organización presentan el mismo riesgo de soborno.

Por ejemplo, pueden presentar mayor exposición:

- Contrataciones públicas.
- Compras.
- Ventas mediante intermediarios.
- Gestión de permisos.
- Relaciones con funcionarios públicos.
- Selección de proveedores.
- Gestión de donaciones.
- Regalos y hospitalidad.

- Operaciones en determinados países o regiones.
- Contratos de alto valor.

Por esta razón, **los procesos con mayor exposición al riesgo pueden requerir una atención de auditoría mayor o más frecuente**.

Resultados de auditorías anteriores

Al elaborar el programa de auditoría deben considerarse también los **resultados de auditorías anteriores**. Si una auditoría previa detectó problemas importantes en el proceso de contratación, la organización debería prestar especial atención a ese proceso en auditorías posteriores.

Esto permite establecer un ciclo:

Auditar → detectar problemas → aplicar acciones correctivas → verificar → volver a evaluar.

De esta manera, la auditoría se convierte en una herramienta de **mejora continua**.

Objetivos de cada auditoría

Cada auditoría debería tener objetivos claramente definidos. Por ejemplo:

Determinar si los controles financieros establecidos para pagos de alto riesgo se aplican correctamente.

Evaluar el cumplimiento de los procedimientos de debida diligencia de proveedores.

Verificar la aplicación de la política sobre regalos y hospitalidad.

Evaluar la gestión de las comunicaciones recibidas mediante el canal de denuncia.

Verificar si las acciones correctivas de una auditoría anterior fueron eficaces.

Tener objetivos claros evita que la auditoría se convierta en una revisión general sin una finalidad concreta.

Criterios de auditoría

Los **criterios de auditoría** son los requisitos utilizados para comparar las evidencias obtenidas.

Pueden incluir:

- Requisitos de ISO 37001.
- Política antisoborno.
- Procedimientos internos.
- Código de conducta.

- Controles financieros.
- Procedimientos de compras.
- Requisitos contractuales.
- Requisitos legales aplicables.

El auditor debe poder explicar **contra qué requisito se está evaluando una determinada situación**.

Alcance de la auditoría

El alcance determina qué será evaluado. Puede incluir:

- Una determinada área.
- Un proceso.
- Una sede.
- Un proyecto.
- Un grupo de proveedores.
- Un período determinado.
- Una operación específica.
- Todo el Sistema de Gestión Antisoborno.

Por ejemplo, una auditoría puede tener como alcance:

"Proceso de selección y contratación de proveedores durante el período enero-junio de 2026." Esto permite definir claramente qué información será revisada.

Evidencia de auditoría

La auditoría debe basarse en **evidencias objetivas**.

Pueden utilizarse:

- Documentos.
- Registros.
- Contratos.
- Facturas.
- Correos corporativos.
- Entrevistas.
- Registros de capacitación.
- Autorizaciones.
- Informes.
- Registros de debida diligencia.
- Evidencias de controles financieros.
- Registros de denuncias cuando corresponda.

La evidencia debe ser suficiente y pertinente para sustentar las conclusiones de la auditoría.

Técnicas de auditoría

Durante una auditoría pueden utilizarse diferentes técnicas.

Entre ellas:

Revisión documental: análisis de políticas, procedimientos y registros.

Entrevistas: conversaciones con trabajadores y responsables de procesos.

Observación: comprobación de cómo se ejecuta realmente una actividad.

Muestreo: revisión de una selección de operaciones o documentos.

Seguimiento de transacciones: análisis de una operación desde su inicio hasta su aprobación y registro.

Comparación: contraste entre procedimientos establecidos y prácticas reales.

La combinación de diferentes técnicas permite obtener una visión más completa.

Muestreo

En organizaciones con un gran número de operaciones, normalmente no resulta necesario revisar absolutamente todas las transacciones.

Puede utilizarse un **muestreo**, seleccionando operaciones que permitan obtener información representativa o que presenten características de mayor riesgo.

Por ejemplo, pueden seleccionarse:

- Pagos de importes elevados.
- Operaciones con terceros de alto riesgo.
- Pagos excepcionales.
- Operaciones aprobadas mediante procedimientos especiales.
- Transacciones relacionadas con funcionarios públicos.
- Operaciones realizadas durante períodos específicos.

La metodología de muestreo debe ser adecuada al objetivo de la auditoría.

Entrevistas a trabajadores

Las entrevistas pueden ayudar a determinar **cómo funcionan realmente los controles**. Por ejemplo, un procedimiento puede establecer que todos los regalos recibidos deben registrarse.

El auditor puede preguntar:

¿Conoce este procedimiento?

¿Dónde se registran los regalos?

¿Qué debe hacer un trabajador cuando recibe un regalo?

¿Quién revisa el registro?

¿Qué ocurre si el regalo supera el límite establecido?

Las respuestas pueden revelar diferencias entre **el procedimiento documentado y la práctica real**.

Verificación de controles financieros

La auditoría puede revisar si los controles financieros diseñados para prevenir sobornos están funcionando.

Por ejemplo:

- Separación de funciones.
- Aprobación de pagos.
- Autorizaciones.
- Documentación de gastos.
- Control de caja.
- Revisión de facturas.
- Control de proveedores.
- Conciliaciones.
- Gestión de pagos excepcionales.

El objetivo no es realizar necesariamente una auditoría financiera completa, sino evaluar **los controles relacionados con el riesgo de soborno**.

Verificación de controles no financieros

ISO 37001 también contempla controles no financieros.

Pueden incluir:

- Procesos de compras.
- Selección de proveedores.
- Contratación de agentes.
- Gestión de recursos humanos.
- Procesos de ventas.
- Contrataciones.
- Evaluación de socios de negocio.
- Gestión de regalos.
- Donaciones.
- Patrocinios.

La auditoría debe considerar que **el riesgo de soborno no se controla únicamente mediante mecanismos contables**.

Auditoría de socios de negocio

Los socios de negocio pueden representar una fuente importante de riesgo.

Por ello, una auditoría puede verificar:

Si se realizó la debida diligencia requerida.

Si existen contratos adecuados.

Si el tercero aceptó las obligaciones antisoborno correspondientes.

Si los controles establecidos se están aplicando.

Si existen señales de alerta que requieren una revisión adicional.

Esto resulta especialmente relevante cuando terceros actúan en nombre de la organización.

Auditoría de la política antisoborno

La auditoría puede comprobar que la política antisoborno:

- Está aprobada.
- Se encuentra disponible.
- Ha sido comunicada.
- Es conocida por el personal correspondiente.
- Es coherente con los riesgos de la organización.
- Se aplica en la práctica.

Pero **tener una política publicada no demuestra por sí solo que el sistema sea eficaz**.

Debe existir evidencia de implementación.

Auditoría de capacitación

También puede revisarse la capacitación antisoborno.

Por ejemplo:

- ¿Quiénes recibieron capacitación?
- ¿La capacitación corresponde a sus funciones?
- ¿Se identificaron grupos de mayor riesgo?
- ¿Existen registros?
- ¿Se evalúa la comprensión cuando corresponde?
- ¿Se realizan actividades de actualización?

La auditoría puede determinar si la formación establecida por la organización **se está ejecutando conforme a lo planificado**.

Auditoría de canales de denuncia

El auditor puede evaluar si los mecanismos para comunicar preocupaciones funcionan adecuadamente.

Puede revisar:

- Existencia del canal.
- Accesibilidad.
- Comunicación del canal.
- Procedimientos de recepción.
- Confidencialidad.
- Gestión de casos.
- Seguimiento.
- Protección frente a represalias.
- Documentación.

El contenido de las denuncias debe manejarse con especial cuidado y respetando las obligaciones legales y de protección de información.

Auditoría de investigaciones

Cuando han existido incidentes, la auditoría puede revisar si la organización los gestionó de acuerdo con sus procedimientos.

Puede verificarse:

Cómo se recibió el caso.

Cómo se evaluó.

Quién realizó la investigación.

Qué evidencias fueron analizadas.

Qué conclusiones se obtuvieron.

Qué acciones fueron adoptadas.

Si se realizó seguimiento.

Esto permite evaluar si la organización realmente **responde ante los incidentes identificados**.

Objetividad e imparcialidad

Uno de los elementos especialmente importantes de ISO 37001:2025 es la **objetividad e imparcialidad del proceso de auditoría**.

La norma establece requisitos específicos para garantizar que las auditorías sean realizadas de manera objetiva e imparcial. Entre las posibilidades contempladas se encuentran personal independiente, determinadas funciones internas distintas del área auditada o un tercero apropiado.

Un principio fundamental es:

Una persona no debe auditar su propia área de trabajo.

Por ejemplo, el responsable directo de un proceso no debería realizar por sí mismo la auditoría de ese mismo proceso y evaluar su propia actuación.

Competencia de los auditores

Los auditores deben contar con **competencia adecuada para realizar el trabajo que se les asigna**.

Esto puede incluir conocimientos sobre:

- Auditoría.
- Sistemas de gestión.
- ISO 37001.
- Riesgos de soborno.
- Controles internos.
- Procesos de la organización.

La competencia necesaria dependerá del alcance y complejidad de la auditoría.

Auditoría interna y auditoría externa

No debe confundirse la **auditoría interna** con la auditoría realizada por un organismo de certificación. La auditoría interna es realizada por la propia organización o por una parte externa que actúa en su nombre, con el objetivo de evaluar internamente el sistema.

La auditoría de certificación es realizada por un **organismo de certificación independiente**, dentro del proceso destinado a determinar si la organización cumple los requisitos de la norma para obtener o mantener una certificación.

Por tanto:

Auditoría interna = evaluación del sistema desde dentro de la organización.

Auditoría de certificación = evaluación independiente realizada para el proceso de certificación.

Hallazgos de auditoría

Una auditoría puede generar diferentes resultados. Entre ellos:

Conformidad: el requisito se cumple.

No conformidad: existe un incumplimiento de un requisito aplicable.

Observación o situación que requiere atención: puede señalar una circunstancia que merece seguimiento, dependiendo de la metodología utilizada.

Oportunidad de mejora: existe una posibilidad de mejorar la eficacia o eficiencia del sistema.

La clasificación concreta debe seguir los criterios definidos por la organización y la metodología de auditoría utilizada.

No conformidades

Una no conformidad significa que **no se ha cumplido un requisito**. Por ejemplo, el procedimiento interno establece que determinados proveedores deben someterse a debida diligencia antes de su contratación, pero la revisión de varios expedientes demuestra que el procedimiento no se aplicó.

El auditor debe documentar adecuadamente:

Qué requisito debía cumplirse.

Qué evidencia se encontró.

Cuál es la diferencia entre el requisito y la situación observada.

Informe de auditoría

Los resultados deben quedar documentados en un **informe de auditoría**. Dependiendo del tamaño y complejidad de la organización, el informe puede incluir:

- Objetivo.
- Alcance.
- Criterios.
- Fecha.
- Áreas auditadas.
- Equipo auditor.
- Evidencias revisadas.
- Hallazgos.
- No conformidades.
- Conclusiones.
- Recomendaciones o aspectos de mejora.
- Acciones posteriores.

La documentación constituye evidencia de que el **programa de auditoría fue implementado y que los resultados fueron obtenidos y comunicados**.

Comunicación de los resultados

Los resultados no deben permanecer únicamente con el auditor. ISO 37001:2025 establece que los resultados deben ser comunicados a los responsables pertinentes, a la función antisoborno y a la alta dirección y, cuando corresponda, al órgano de gobierno.

Esto permite que los responsables puedan:

- Analizar los hallazgos.
- Determinar acciones.
- Asignar responsabilidades.
- Establecer plazos.
- Supervisar las mejoras.

Seguimiento de las acciones

Una auditoría no termina necesariamente con la emisión del informe. Cuando existen no conformidades, la organización debe realizar el **seguimiento de las acciones adoptadas**.

Por ejemplo:

Auditoría → hallazgo → análisis de causa → acción correctiva → implementación → verificación de eficacia.

Este proceso permite comprobar que los problemas detectados **no quedan simplemente registrados en un informe**.

Ejemplo práctico: contratación de proveedores

Durante una auditoría interna se selecciona una muestra de 30 expedientes de proveedores. El procedimiento establece que los proveedores considerados de mayor riesgo deben pasar por un proceso de debida diligencia.

El auditor encuentra que:

- 5 expedientes no contienen evidencia suficiente de la evaluación.
- 2 proveedores fueron contratados antes de completar el proceso.
- No existe evidencia de una revisión posterior.

El resultado no debería limitarse a señalar que “faltan documentos”.

La auditoría debe ayudar a determinar:

Por qué no se realizó la debida diligencia.

Quién debía realizarla.

Si el sistema permitía contratar sin completar el control.

Si el problema afecta a otros proveedores.

Qué acción debe adoptarse.

Ejemplo práctico: regalos y hospitalidad

La organización dispone de una política que establece requisitos para aceptar regalos. Durante la auditoría se revisan registros y se descubre que varios trabajadores recibieron regalos, pero no existe evidencia de que hayan sido registrados.

El auditor puede investigar:

- Si los trabajadores conocían la política.
- Si el registro estaba disponible.
- Si existía un responsable.
- Si los límites eran claros.
- Si se realizaba supervisión.

La solución puede requerir **mejorar el procedimiento y la comunicación**, y no simplemente recordar a los trabajadores que deben cumplirlo.

Ejemplo práctico: pagos

La organización exige dos niveles de autorización para determinados pagos. La auditoría selecciona una muestra de operaciones y encuentra pagos que fueron procesados con una sola autorización.

La auditoría debe determinar si:

- Se trató de una excepción autorizada.
- Existió un error.
- El control fue omitido.
- El sistema informático permitió evitarlo.
- El problema es recurrente.
- Existe riesgo de soborno asociado.

De esta manera, la auditoría analiza **el funcionamiento real del control**.

Auditoría como herramienta preventiva

La auditoría interna no debe utilizarse únicamente para detectar problemas después de que hayan ocurrido. También puede identificar **debilidades antes de que se produzca un incidente de soborno**.

Por ejemplo, si se descubre que los proveedores de alto riesgo están siendo contratados sin una evaluación adecuada, la organización puede corregir el problema antes de que exista un pago indebido. Por eso, una auditoría eficaz tiene una función **preventiva, detectiva y de mejora**.

Auditoría y mejora continua

Los resultados de las auditorías constituyen una fuente importante de información para la **mejora continua del Sistema de Gestión Antisoborno**.

Los hallazgos pueden utilizarse para:

- Actualizar procedimientos.
- Mejorar controles.
- Modificar evaluaciones de riesgo.
- Reforzar capacitaciones.
- Mejorar la debida diligencia.
- Revisar responsabilidades.
- Mejorar los canales de denuncia.
- Modificar controles financieros.
- Fortalecer la supervisión.

ISO 37001:2025 contempla la auditoría interna dentro de la evaluación del desempeño y establece además un capítulo específico sobre **mejora**, incluyendo mejora continua y acciones correctivas.

Idea clave

La **auditoría interna no consiste simplemente en revisar documentos**. Su verdadero objetivo es determinar si el Sistema de Gestión Antisoborno **funciona en la práctica, cumple los requisitos establecidos y es capaz de gestionar adecuadamente los riesgos de soborno**.

Una auditoría interna eficaz debe:

Planificarse a intervalos definidos.

Considerar los riesgos y la importancia de los procesos.

Tener objetivos, criterios y alcance claramente establecidos.

Utilizar evidencias objetivas.

Contar con auditores competentes.

Garantizar objetividad e imparcialidad.

Evaluar tanto controles financieros como no financieros.

Considerar los resultados de auditorías anteriores.

Documentar los hallazgos y conclusiones.

Comunicar los resultados a los responsables correspondientes.

Dar seguimiento a las acciones correctivas.

Contribuir a la mejora continua del Sistema de Gestión Antisoborno.

En definitiva, **auditar no significa buscar errores para sancionar personas**. Significa comprobar si el sistema diseñado para prevenir y detectar el soborno realmente funciona y, cuando se encuentran debilidades, utilizar esa información para **fortalecer la organización y reducir el riesgo de que el soborno ocurra**.

6.2. Revisión por la dirección

Introducción

La **revisión por la dirección** es uno de los mecanismos mediante los cuales la alta dirección evalúa si el Sistema de Gestión Antisoborno continúa siendo **adecuado, suficiente y eficaz** para enfrentar los riesgos de soborno de la organización.

De acuerdo con **ISO 37001:2025**, la alta dirección debe revisar el Sistema de Gestión Antisoborno **a intervalos planificados**. La revisión no consiste simplemente en recibir un informe de cumplimiento, sino en analizar información relevante sobre el funcionamiento del sistema y **tomar decisiones sobre su continuidad, mejora o modificación**.

La revisión por la dirección conecta directamente los resultados de las auditorías, las investigaciones, los indicadores, los riesgos y las acciones correctivas con las **decisiones de la alta dirección**.

¿Qué significa “revisión por la dirección”?

La revisión por la dirección es un proceso mediante el cual la **alta dirección analiza el desempeño global del Sistema de Gestión Antisoborno** y determina si este continúa siendo apropiado para la organización. No debe confundirse con una auditoría.

La **auditoría interna** busca obtener evidencias y evaluar el cumplimiento y funcionamiento del sistema.

La **revisión por la dirección** utiliza información procedente de diferentes fuentes para que la alta dirección pueda **evaluar el sistema y tomar decisiones**.

Por ejemplo, una revisión puede comenzar con los resultados de una auditoría que detectó deficiencias en la debida diligencia de proveedores. La dirección debe analizar qué significa este resultado para el sistema y determinar si son necesarias modificaciones, recursos adicionales o nuevas medidas de control.

Responsabilidad de la alta dirección

La responsabilidad principal de la revisión corresponde a la **alta dirección**. Esto es importante porque el Sistema de Gestión Antisoborno no debe funcionar únicamente como una responsabilidad del área de cumplimiento. La dirección debe demostrar que el antisoborno forma parte de la **gestión normal de la organización y de su toma de decisiones**.

Durante la revisión, la alta dirección puede analizar:

- Resultados de auditorías.
- Incidentes y denuncias.
- Investigaciones realizadas.
- No conformidades.
- Acciones correctivas.
- Evolución de los riesgos de soborno.
- Resultados de seguimiento y medición.
- Cambios en el entorno de la organización.
- Necesidades de las partes interesadas.
- Oportunidades de mejora.

Participación del órgano de gobierno

Cuando la organización cuenta con un **órgano de gobierno**, ISO 37001:2025 establece además que este debe realizar revisiones, a intervalos planificados, sobre la implementación del Sistema de Gestión Antisoborno por parte de la alta dirección.

Esta revisión se basa en la información proporcionada por la alta dirección, la función antisoborno y cualquier otra información que el órgano de gobierno solicite u obtenga.

Por tanto, debe distinguirse entre:

Alta dirección: revisa el Sistema de Gestión Antisoborno y toma decisiones sobre su desempeño y mejora.

Órgano de gobierno: supervisa la implementación del sistema por parte de la alta dirección, cuando dicho órgano exista.

¿Con qué frecuencia debe realizarse?

La norma exige que la revisión se realice **a intervalos planificados**, pero no establece una única frecuencia universal aplicable a todas las organizaciones. La organización debe determinar una frecuencia adecuada teniendo en cuenta factores como:

- Tamaño de la organización.
- Complejidad de sus operaciones.
- Nivel de riesgo de soborno.
- Cambios importantes en sus actividades.
- Resultados de auditorías.
- Incidentes ocurridos.
- Cambios legales o regulatorios.
- Resultados de revisiones anteriores.

Una organización puede establecer, por ejemplo, una revisión formal **una vez al año**, complementada con revisiones extraordinarias cuando ocurra una situación importante. Lo importante es que exista una **planificación definida y evidencia de que la revisión realmente se realiza**.

Entradas de la revisión por la dirección

ISO 37001:2025 establece diferentes elementos que deben ser considerados durante la revisión.

Entre ellos se encuentran:

- Estado de las acciones derivadas de revisiones anteriores.
- Cambios en cuestiones internas y externas relevantes.
- Cambios en las necesidades y expectativas de las partes interesadas.
- Desempeño del Sistema de Gestión Antisoborno.
- Resultados de seguimiento y medición.
- Resultados de auditorías.
- No conformidades y acciones correctivas.
- Informes de soborno.
- Investigaciones.
- Naturaleza y extensión de los riesgos de soborno.
- Eficacia de las medidas adoptadas para tratar los riesgos.
- Oportunidades de mejora continua.

Esto significa que la revisión debe ser **basada en información objetiva y relevante**, y no únicamente en una opinión general de la dirección.

Estado de las acciones de revisiones anteriores

La primera cuestión que puede analizarse es qué ocurrió con las decisiones adoptadas durante revisiones anteriores.

Por ejemplo, si la dirección decidió:

“Implementar un nuevo procedimiento de debida diligencia para proveedores de alto riesgo”,

la siguiente revisión debería analizar:

- Si el procedimiento fue elaborado.
- Si fue aprobado.
- Si fue implementado.
- Si los trabajadores fueron capacitados.
- Si se está utilizando.
- Si produjo mejoras.
- Si todavía existen deficiencias.

De esta manera, las decisiones tomadas anteriormente **no quedan simplemente registradas en un acta**, sino que reciben seguimiento.

Cambios internos y externos

La organización debe analizar si se han producido cambios que puedan afectar al Sistema de Gestión Antisoborno. Los cambios internos pueden incluir:

- Reestructuración de la organización.
- Nuevas áreas.
- Nuevos responsables.
- Expansión de operaciones.
- Nuevos productos o servicios.
- Cambios en procesos de contratación.
- Incorporación de nuevos socios de negocio.

Los cambios externos pueden incluir:

- Nuevas leyes.
- Cambios regulatorios.
- Nuevas exigencias de clientes.
- Cambios en los mercados.
- Nuevos riesgos en determinados países o sectores.
- Cambios en las relaciones con autoridades públicas.

La finalidad es determinar si el sistema continúa siendo **adecuado para el contexto actual de la organización**.

Necesidades y expectativas de las partes interesadas

ISO 37001:2025 incorpora expresamente en las entradas de la revisión los **cambios en las necesidades y expectativas de las partes interesadas** que sean relevantes para el Sistema de Gestión Antisoborno.

Entre las partes interesadas pueden encontrarse, según el contexto de la organización:

- Clientes.
- Trabajadores.
- Proveedores.
- Socios de negocio.
- Accionistas.
- Autoridades.
- Entidades reguladoras.
- Comunidades u otras partes relevantes.

La dirección debe evaluar si los cambios en estas relaciones generan **nuevas obligaciones, expectativas o riesgos antisoborno**.

Desempeño del Sistema de Gestión Antisoborno

La dirección debe analizar información sobre el **desempeño del sistema**.

Esto permite responder preguntas como:

¿Los controles están funcionando?

¿Se están cumpliendo los procedimientos?

¿Los riesgos están disminuyendo?

¿Existen problemas recurrentes?

¿Las acciones correctivas están funcionando?

¿Se están produciendo nuevos incidentes?

El objetivo es pasar de una percepción subjetiva a una evaluación basada en **datos, evidencias y tendencias**.

No conformidades y acciones correctivas

La dirección debe revisar las tendencias relacionadas con las **no conformidades y acciones correctivas**. Por ejemplo, si durante un año se identificaron diez no conformidades y ocho estuvieron relacionadas con proveedores, esto puede indicar que existe una debilidad específica en el proceso de gestión de terceros.

La dirección puede entonces decidir:

- Revisar el procedimiento.
- Aumentar los controles.
- Mejorar la capacitación.
- Modificar responsabilidades.
- Aumentar la supervisión.
- Revaluar los riesgos.

La importancia no está únicamente en **cuántas no conformidades existen**, sino en identificar patrones y causas.

Resultados de seguimiento y medición

La revisión debe considerar los resultados obtenidos mediante las actividades de **seguimiento y medición**. Dependiendo del sistema establecido por la organización, pueden utilizarse indicadores relacionados con:

- Capacitación antisoborno.
- Debida diligencia.
- Evaluaciones de proveedores.
- Denuncias recibidas.
- Tiempo de tratamiento de casos.
- Investigaciones.
- Acciones correctivas.
- Auditorías.
- Controles financieros.
- Incidentes.
- Cumplimiento de procedimientos.

Los indicadores deben servir para **comprender el comportamiento del sistema**, no simplemente para generar estadísticas.

Resultados de las auditorías

Los resultados de las **auditorías internas** constituyen una entrada importante para la revisión por la dirección.

La alta dirección puede analizar:

- Número de hallazgos.
- No conformidades.
- Áreas con problemas recurrentes.
- Controles que presentan debilidades.
- Acciones correctivas pendientes.
- Resultados de auditorías anteriores.
- Evolución de los hallazgos.

Por ejemplo, si tres auditorías consecutivas detectan deficiencias en la aprobación de pagos, puede existir un problema estructural que requiere una decisión de la dirección.

Informes de soborno

La revisión debe considerar también los **informes de posibles actos de soborno**.

Esto permite evaluar:

- Cantidad de reportes.
- Naturaleza de las situaciones comunicadas.
- Áreas involucradas.
- Tendencias.
- Tipos de conducta reportados.
- Resultado de las investigaciones.

Un aumento de reportes no significa necesariamente que el sistema esté empeorando. Puede significar que **los trabajadores están utilizando mejor los canales de denuncia y que la organización está detectando situaciones que anteriormente permanecían ocultas**. Por eso, los datos deben interpretarse dentro de su contexto.

Investigaciones

La dirección también debe considerar información relacionada con las **investigaciones de incidentes**.

Puede analizar:

- Qué tipos de incidentes ocurrieron.
- Qué áreas estuvieron involucradas.
- Qué causas fueron identificadas.
- Qué controles fallaron.
- Qué acciones correctivas se adoptaron.
- Si los incidentes se repitieron.

La finalidad es obtener una visión global y determinar si existen **problemas sistémicos**.

Riesgos de soborno

Uno de los elementos fundamentales de la revisión es la evaluación de la **naturaleza y extensión de los riesgos de soborno que enfrenta la organización**.

La dirección puede preguntarse:

¿Han aparecido nuevos riesgos?

¿Han aumentado determinados riesgos?

¿Han disminuido algunos riesgos?

¿Existen nuevos terceros de alto riesgo?

¿La organización ha comenzado a operar en nuevos mercados?

¿Existen nuevas relaciones con funcionarios públicos?

¿Los controles existentes siguen siendo suficientes?

Esto permite conectar directamente la revisión por la dirección con la **gestión de riesgos antisoborno**.

Eficacia de las medidas adoptadas

No basta con implementar controles. La dirección debe analizar si las medidas adoptadas para tratar los riesgos de soborno son **eficaces**. Por ejemplo, una organización puede haber establecido un procedimiento de debida diligencia para proveedores.

La pregunta no debe ser únicamente:

"¿Tenemos el procedimiento?"

Debe ser:

"¿El procedimiento está reduciendo eficazmente el riesgo que pretendemos controlar?"

Esta diferencia es fundamental para evaluar la verdadera eficacia del sistema.

Oportunidades de mejora

La revisión también debe identificar **oportunidades de mejora continua**.

Estas pueden estar relacionadas con:

- Procesos.
- Controles.
- Tecnología.
- Capacitación.
- Gestión de proveedores.
- Evaluación de riesgos.
- Canales de denuncia.
- Comunicación.
- Auditorías.
- Documentación.

Una oportunidad de mejora no necesariamente significa que exista una no conformidad. Puede significar que **algo funciona, pero podría funcionar mejor**.

Resultados de la revisión

La revisión por la dirección debe producir **resultados concretos**. ISO 37001:2025 establece que estos resultados deben incluir decisiones relacionadas con:

Oportunidades de mejora continua.

Necesidades de cambios en el Sistema de Gestión Antisoborno.

Por ejemplo, la dirección puede decidir:

- Modificar un procedimiento.
- Aumentar recursos.
- Implementar nuevos controles.
- Cambiar responsabilidades.
- Actualizar la evaluación de riesgos.
- Mejorar la capacitación.
- Realizar una auditoría adicional.
- Revisar determinados proveedores.
- Implementar nuevas herramientas tecnológicas.

La revisión debe generar decisiones

Una reunión en la que la dirección simplemente recibe información no constituye, por sí sola, una revisión eficaz. Debe existir un proceso de **análisis y toma de decisiones**.

Por ejemplo:

Problema identificado: numerosos proveedores de alto riesgo no tienen una debida diligencia actualizada.

Análisis: el procedimiento no establece claramente cuándo debe actualizarse la evaluación.

Decisión: modificar el procedimiento y establecer una revisión periódica.

Responsable: área correspondiente.

Plazo: fecha definida.

Seguimiento: verificar la implementación durante la siguiente revisión.

Este enfoque convierte la revisión en una herramienta de **gestión activa**.

Información documentada

La organización debe conservar **información documentada como evidencia de los resultados de las revisiones por la dirección**.

Esto puede materializarse mediante:

- Acta de reunión.
- Informe de revisión.
- Registro de decisiones.
- Matriz de acciones.
- Presentación formal.
- Informe de desempeño.
- Registro de seguimiento.

La documentación debe permitir demostrar **qué se revisó, qué se decidió y qué acciones fueron determinadas**.

Ejemplo práctico

Una empresa realiza su revisión anual del Sistema de Gestión Antisoborno. Durante la revisión se presentan los siguientes resultados:

Auditorías: tres no conformidades relacionadas con proveedores.

Denuncias: aumento de comunicaciones relacionadas con regalos.

Investigaciones: un caso confirmado de incumplimiento de los procedimientos internos.

Riesgos: aumento de la exposición debido a nuevos contratos con entidades públicas.

Capacitación: 95 % del personal completó la formación requerida.

La dirección analiza esta información y determina que el sistema funciona, pero necesita fortalecerse en determinadas áreas.

Como resultado, decide:

Actualizar el procedimiento de debida diligencia.

Reforzar los controles sobre regalos y hospitalidad.

Realizar capacitación adicional para las áreas de mayor riesgo.

Revisar los controles relacionados con contrataciones públicas.

Realizar seguimiento específico durante el siguiente período.

Este ejemplo demuestra cómo los diferentes elementos del sistema pueden convertirse en **decisiones concretas de la dirección**.

Revisión extraordinaria

Aunque existan revisiones planificadas, determinadas situaciones pueden justificar una revisión adicional.

Por ejemplo:

- Un incidente grave de soborno.
- Una modificación importante de la estructura organizativa.
- Entrada en un nuevo mercado de alto riesgo.
- Una adquisición empresarial.
- Cambios legales importantes.
- Aparición de nuevos riesgos significativos.
- Resultados negativos de una auditoría.

En estas circunstancias, esperar hasta la siguiente revisión programada podría no ser adecuado.

Relación con la auditoría interna

La auditoría interna y la revisión por la dirección están estrechamente relacionadas, pero cumplen funciones diferentes.

La auditoría genera evidencias y hallazgos.

La revisión por la dirección analiza esos resultados junto con otra información relevante.

La dirección toma decisiones.

Las decisiones generan acciones.

Las acciones son posteriormente verificadas.

Por ello, puede representarse el proceso de manera sencilla:

Auditoría → resultados → revisión por la dirección → decisiones → acciones → seguimiento → mejora.

Relación con la mejora continua

La revisión por la dirección constituye uno de los mecanismos que permiten que el Sistema de Gestión Antisoborno **evolucione con la organización**. Los riesgos cambian, las operaciones cambian, los proveedores cambian, las leyes pueden cambiar y también pueden cambiar las expectativas de las partes interesadas. Por ello, un sistema antisoborno no debe permanecer estático.

La revisión permite determinar si es necesario **adaptar el sistema a las nuevas circunstancias**.

Idea clave

La **revisión por la dirección** es mucho más que una reunión periódica de la gerencia. Es un proceso formal mediante el cual la alta dirección evalúa si el Sistema de Gestión Antisoborno continúa siendo **adecuado, suficiente y eficaz**, utilizando información sobre auditorías, riesgos, investigaciones, denuncias, indicadores, no conformidades, acciones correctivas y cambios relevantes.

Una revisión eficaz debe:

Realizarse a intervalos planificados.

Contar con la participación de la alta dirección.

Considerar información objetiva sobre el desempeño del sistema.

Analizar los cambios internos y externos relevantes.

Considerar los cambios en las necesidades y expectativas de las partes interesadas.

Revisar los riesgos de soborno.

Analizar los resultados de auditorías e investigaciones.

Evaluar la eficacia de las medidas adoptadas.

Identificar oportunidades de mejora.

Generar decisiones y acciones concretas.

Conservar información documentada como evidencia de los resultados.

En definitiva, **la dirección debe utilizar los resultados del Sistema de Gestión Antisoborno para tomar decisiones**. De esta manera, la revisión por la dirección se convierte en un mecanismo que conecta el desempeño del sistema con la **gestión estratégica de la organización y su mejora continua**.

6.3. Acciones correctivas

Introducción

Las **acciones correctivas** forman parte fundamental de la mejora del Sistema de Gestión Antisoborno. Su finalidad no es únicamente solucionar un problema que ya ocurrió, sino **identificar y tratar sus causas para reducir la posibilidad de que vuelva a ocurrir o que una situación similar aparezca en otra parte de la organización**.

En la versión vigente **ISO 37001:2025**, el tratamiento de las no conformidades y las acciones correctivas se encuentra en el **apartado 10.2**, dentro del capítulo de mejora. La norma establece que, cuando ocurre una no conformidad, la organización debe reaccionar ante ella, controlar y corregir la situación cuando corresponda, tratar sus consecuencias, analizar sus causas, implementar las acciones necesarias y posteriormente **revisar la eficacia de las acciones correctivas adoptadas**.

Por ello, una acción correctiva no debe entenderse simplemente como **"arreglar un error"**. Se trata de un proceso estructurado para comprender por qué ocurrió el problema y fortalecer el sistema.

¿Qué es una no conformidad?

Una **no conformidad** es el incumplimiento de un requisito aplicable. En un Sistema de Gestión Antisoborno, el requisito puede proceder de diferentes fuentes:

- ISO 37001.
- Política antisoborno.
- Procedimientos internos.
- Controles establecidos por la organización.
- Requisitos contractuales.
- Obligaciones legales aplicables.
- Requisitos establecidos para determinados procesos.

Por ejemplo, si la organización establece que determinados proveedores deben completar una evaluación de debida diligencia antes de ser contratados y se descubre que un proveedor fue contratado sin realizarla, puede existir una **no conformidad respecto del procedimiento establecido**.

Una no conformidad no significa necesariamente que exista soborno

Es importante diferenciar ambos conceptos. Una **no conformidad** significa que un requisito no se cumplió. Un **acto de soborno** implica una conducta de soborno que debe evaluarse de acuerdo con los hechos y las normas aplicables. Por ejemplo, si un trabajador omite una autorización obligatoria para un pago, existe una posible **no conformidad del control establecido**, aunque no necesariamente haya existido un soborno.

Por el contrario, puede existir un posible acto de soborno incluso cuando los documentos formales aparentemente cumplen los procedimientos.

Por esta razón, las acciones correctivas deben centrarse en **las deficiencias del sistema**, mientras que los posibles actos de soborno pueden requerir además una investigación específica.

¿Cuándo puede ser necesaria una acción correctiva?

Una acción correctiva puede resultar necesaria cuando se detecta:

- Una no conformidad durante una auditoría.
- Incumplimiento de un procedimiento.
- Una debilidad importante de control.
- Un incidente relacionado con soborno.
- Un problema repetitivo.
- Una deficiencia detectada durante una investigación.
- Incumplimiento de un requisito establecido por la organización.
- Una situación que demuestra que un control no está funcionando como estaba previsto.

La respuesta debe ser **proporcional a la naturaleza y los efectos de la no conformidad**. ISO 37001:2025 establece expresamente este principio de proporcionalidad.

Primer paso: reaccionar ante la no conformidad

Cuando se detecta una no conformidad, la organización debe **reaccionar de manera oportuna**.

Esto puede implicar:

Controlar la situación.

Corregir el problema.

Detener una operación cuando sea necesario.

Evitar que el problema continúe produciendo efectos.

Tratar las consecuencias derivadas de la situación.

Por ejemplo, si se descubre que un pago fue procesado sin la autorización requerida, puede ser necesario detener pagos posteriores relacionados con la misma operación mientras se analiza la situación.

Corrección y acción correctiva

Es importante diferenciar **corrección** de **acción correctiva**.

La **corrección** busca solucionar el problema inmediato.

La **acción correctiva** busca tratar la causa del problema para evitar su repetición.

Por ejemplo:

Problema: un proveedor fue contratado sin completar la debida diligencia.

Corrección: completar la evaluación del proveedor y regularizar el expediente.

Acción correctiva: modificar el proceso de contratación para impedir que el sistema permita contratar a proveedores de alto riesgo antes de completar la debida diligencia.

La primera actuación **soluciona el caso concreto**.

La segunda busca **evitar que vuelva a ocurrir**.

Tratar las consecuencias

La organización también debe considerar las **consecuencias de la no conformidad**.

Dependiendo de la situación, pueden existir consecuencias:

- Financieras.
- Contractuales.
- Operativas.
- Reputacionales.
- Disciplinarias.
- Legales.
- Relacionadas con terceros.

Por ejemplo, si se realizó un pago que no estaba correctamente autorizado, no basta con corregir el registro interno. La organización debe evaluar si el pago debe ser recuperado, investigado o sometido a otras medidas de acuerdo con las circunstancias.

Analizar la causa de la no conformidad

Uno de los elementos más importantes de una acción correctiva es **determinar por qué ocurrió el problema**.

Preguntar únicamente:

“¿Quién cometió el error?”

normalmente no es suficiente.

Es necesario analizar:

¿Por qué el control no funcionó?

¿Por qué la persona pudo realizar la operación?

¿El procedimiento era claro?

¿La persona conocía el procedimiento?

¿Existía capacitación suficiente?

¿Existía supervisión?

¿El sistema informático permitía evitar el control?

¿La responsabilidad estaba claramente asignada?

¿El problema podía ocurrir en otras áreas?

Estas preguntas permiten pasar de una respuesta superficial a un **análisis de causa**.

Análisis de causa raíz

El **análisis de causa raíz** busca identificar los factores que permitieron que ocurriera la no conformidad.

Por ejemplo:

No conformidad: se aprobó un pago sin la segunda autorización requerida.

Causa inmediata: el pago fue aprobado por una sola persona.

Causa del proceso: el procedimiento permitía procesar excepcionalmente el pago sin una segunda aprobación.

Causa del sistema: el sistema informático no impedía completar la operación.

Causa organizacional: no existía una revisión periódica de las excepciones.

En este caso, simplemente capacitar nuevamente al trabajador podría no ser suficiente.

La organización podría necesitar **modificar el procedimiento y el control informático**.

Determinar si existen casos similares

ISO 37001:2025 exige que la organización determine si existen **no conformidades similares o si podrían ocurrir en otras partes de la organización**. Este aspecto es especialmente importante.

Si se detecta que un proveedor fue contratado sin debida diligencia, no debería revisarse únicamente ese proveedor.

La organización puede preguntarse:

¿Cuántos proveedores fueron contratados mediante el mismo procedimiento?

¿Existe el mismo problema en otras áreas?

¿El mismo control se aplica de la misma manera en otras sedes?

¿Existen otros procesos donde pueda ocurrir la misma situación?

Esto permite evitar que la acción correctiva sea demasiado limitada.

Implementación de la acción correctiva

Una vez identificada la causa, la organización debe **implementar las acciones necesarias**.

Estas pueden incluir:

- Modificación de procedimientos.
- Nuevos controles.
- Cambios en las autorizaciones.
- Separación de funciones.
- Capacitación.
- Revisión de responsabilidades.
- Mejoras tecnológicas.
- Revisión de proveedores.
- Refuerzo de la supervisión.
- Actualización de la evaluación de riesgos.

La acción elegida debe estar relacionada con la **causa identificada**.

No todas las acciones correctivas son iguales

La respuesta debe ser proporcional al problema. Un incumplimiento menor y aislado puede requerir una corrección y una mejora específica. Una deficiencia repetitiva en un proceso crítico puede requerir una modificación estructural.

Por ejemplo:

Problema menor: un registro fue completado incorrectamente una vez.

Problema sistémico: el 30 % de los expedientes revisados presentan el mismo defecto.

En el segundo caso, simplemente recordar al personal que complete correctamente los registros probablemente **no sea suficiente**.

Responsabilidades

Toda acción correctiva debería tener claramente definido:

Qué debe hacerse.

Quién es responsable.

Cuándo debe completarse.

Qué recursos son necesarios.

Cómo se verificará su implementación.

Cómo se evaluará su eficacia.

Esto evita que las acciones correctivas queden como recomendaciones generales sin seguimiento.

Plazos

Las acciones correctivas deben gestionarse dentro de **plazos razonables y definidos**.

El plazo puede depender de:

- Gravedad de la no conformidad.
- Riesgo de soborno.
- Consecuencias existentes.
- Complejidad de la solución.
- Recursos necesarios.
- Riesgo de repetición.

Una situación que presenta un riesgo elevado puede requerir medidas inmediatas, mientras que una modificación estructural puede necesitar un período mayor de implementación.

Verificación de la implementación

Una vez transcurrido el plazo, debe verificarse si la acción correctiva fue realmente implementada. Por ejemplo, si la organización decidió modificar el procedimiento de aprobación de pagos, debe comprobarse:

¿El procedimiento fue actualizado?

¿Fue aprobado?

¿Fue comunicado?

¿Los trabajadores recibieron la información necesaria?

¿El nuevo control está funcionando?

La implementación documental por sí sola no demuestra necesariamente que la acción haya sido eficaz.

Evaluación de la eficacia

Uno de los requisitos fundamentales de ISO 37001:2025 es **revisar la eficacia de las acciones correctivas adoptadas**.

La pregunta fundamental es:

¿La acción realmente solucionó la causa del problema?

Por ejemplo, una organización detecta que algunos proveedores fueron contratados sin debida diligencia y establece un nuevo procedimiento. Después de varios meses puede revisarse una muestra de nuevas contrataciones. Si todos los proveedores correspondientes fueron evaluados correctamente, existe evidencia de que el control puede estar funcionando.

Si el mismo problema continúa apareciendo, la acción correctiva **no fue suficientemente eficaz** y será necesario revisar nuevamente las causas y las medidas adoptadas.

Indicadores de eficacia

Dependiendo del caso, la eficacia puede evaluarse mediante:

- Reducción de no conformidades similares.
- Cumplimiento de nuevos controles.
- Resultados de auditorías posteriores.
- Reducción de excepciones.
- Cumplimiento de procedimientos.
- Resultados de revisiones de expedientes.
- Disminución de incidentes relacionados.
- Mejora de indicadores de cumplimiento.

La metodología debe adaptarse a la naturaleza de la acción.

Documentación de las acciones correctivas

ISO 37001:2025 requiere conservar **información documentada como evidencia de la naturaleza de las no conformidades, las acciones adoptadas y los resultados de las acciones correctivas**.

La documentación puede incluir:

- Descripción de la no conformidad.
- Evidencias.
- Análisis de causas.
- Consecuencias identificadas.
- Corrección realizada.
- Acción correctiva.
- Responsable.
- Fecha prevista.
- Evidencia de implementación.

- Resultado de la verificación.
- Evaluación de eficacia.

Esta información permite demostrar que la organización **no ignoró el problema y realizó un tratamiento estructurado**.

Relación con las auditorías internas

Las acciones correctivas están estrechamente relacionadas con las **auditorías internas**. Una auditoría puede detectar una no conformidad.

Después:

Se registra la no conformidad.

Se analiza su causa.

Se determina una acción correctiva.

Se implementa la acción.

Se verifica su eficacia.

La auditoría posterior puede comprobar si el problema fue solucionado.

De esta forma, la auditoría y las acciones correctivas forman parte de un mismo ciclo de mejora.

Relación con la revisión por la dirección

Los resultados de las acciones correctivas también pueden ser relevantes para la **revisión por la dirección**.

La dirección puede analizar:

- Número de acciones correctivas.
- Acciones pendientes.
- Acciones vencidas.
- Problemas recurrentes.
- Causas comunes.
- Eficacia de las medidas.
- Recursos necesarios.

Si se detecta que un mismo tipo de no conformidad aparece repetidamente, la dirección puede decidir **modificar el sistema, aumentar recursos o establecer nuevos controles**.

Acciones correctivas y gestión de riesgos

Las acciones correctivas también deben relacionarse con la **evaluación de riesgos de soborno**. Si un incidente demuestra que determinado riesgo estaba subestimado, la organización puede necesitar revisar su evaluación.

Por ejemplo:

Riesgo identificado: pagos indebidos a intermediarios.

Incidente: se detecta una operación sospechosa.

Análisis: los controles existentes eran insuficientes para determinadas operaciones.

Acción correctiva: reforzar la aprobación y debida diligencia de intermediarios.

Resultado: actualizar la evaluación del riesgo y los controles asociados.

Así, una acción correctiva puede generar cambios no solamente en un procedimiento, sino también en la **gestión global del riesgo antisoborno**.

Ejemplo práctico: proveedor de alto riesgo

Una organización detecta que tres proveedores fueron contratados sin completar la debida diligencia requerida. La primera reacción consiste en revisar inmediatamente los tres expedientes.

Posteriormente se realiza un análisis y se descubre que el procedimiento de compras **no bloquea la contratación cuando la evaluación de riesgo está pendiente**. La organización determina las siguientes acciones:

Corrección: completar la debida diligencia de los proveedores afectados.

Análisis de causa: debilidad del proceso de contratación.

Acción correctiva: modificar el procedimiento y establecer un control obligatorio antes de la contratación.

Medida adicional: capacitar al personal de compras.

Verificación: revisar posteriormente una muestra de nuevas contrataciones.

Evaluación de eficacia: comprobar si el problema vuelve a aparecer.

Este ejemplo muestra claramente la diferencia entre **solucionar el caso y corregir la causa**.

Ejemplo práctico: regalos y hospitalidad

Durante una auditoría se detecta que varios trabajadores no registraron regalos recibidos de proveedores.

La organización analiza el problema y descubre que:

- El registro no era fácilmente accesible.
- Los trabajadores desconocían determinados requisitos.
- No existía una revisión periódica del registro.

Las acciones pueden incluir:

Mejorar el procedimiento.

Simplificar el mecanismo de registro.

Capacitar al personal correspondiente.

Establecer una revisión periódica.

Posteriormente se verifica si los nuevos controles están funcionando.

Ejemplo práctico: pagos

Una auditoría detecta que varios pagos de alto riesgo fueron aprobados sin la revisión independiente requerida. El análisis demuestra que el sistema permitía continuar la operación aunque faltara la segunda autorización. La organización decide implementar un **bloqueo automático** hasta completar la autorización correspondiente. Esta solución es más sólida que limitarse a enviar un correo recordatorio a los trabajadores, porque **modifica el mecanismo de control que permitió que ocurriera la no conformidad**.

Acción correctiva frente a un problema repetitivo

Cuando una organización detecta la misma no conformidad varias veces, debe prestar especial atención.

La repetición puede indicar que:

La causa no fue correctamente identificada.

La acción correctiva fue insuficiente.

La acción no fue implementada correctamente.

El control diseñado no es adecuado.

Existe un problema más amplio dentro del sistema.

En estos casos, puede ser necesario realizar un nuevo análisis y adoptar una acción más profunda.

Errores frecuentes en las acciones correctivas

Uno de los errores más comunes consiste en confundir **capacitación con solución**. Por ejemplo, si un procedimiento permite realizar un pago sin autorización suficiente, capacitar nuevamente al trabajador puede ser útil, pero no necesariamente elimina la causa.

Otro error consiste en **corregir únicamente el caso individual** sin revisar si existen situaciones similares. También es frecuente cerrar una acción simplemente porque se modificó un documento, sin comprobar si el nuevo procedimiento **se está aplicando y funciona eficazmente**.

Enfoque correcto

Un enfoque adecuado puede resumirse de la siguiente manera:

Detectar → contener → corregir → analizar causas → comprobar casos similares → actuar → verificar → evaluar eficacia → mejorar el sistema.

Este ciclo permite que una no conformidad se convierta en una **fuente de aprendizaje y fortalecimiento del Sistema de Gestión Antisoborno**.

Relación con la mejora continua

En **ISO 37001:2025**, la mejora continua y las acciones correctivas aparecen como elementos relacionados dentro del capítulo 10, aunque actualmente se encuentran en apartados diferentes: **10.1 Mejora continua** y **10.2 No conformidad y acción correctiva**.

Esto es importante porque la organización no debe limitarse a reaccionar ante los problemas.

Debe utilizar la información obtenida de:

- Auditorías.
- Incidentes.
- Investigaciones.
- No conformidades.
- Acciones correctivas.
- Evaluaciones de riesgos.
- Revisiones por la dirección.

para **mejorar continuamente la idoneidad, adecuación y eficacia del Sistema de Gestión Antisoborno**.

Idea clave

Las **acciones correctivas no consisten simplemente en solucionar un error**. Su propósito es comprender la causa de una no conformidad, controlar sus consecuencias, evitar su repetición y fortalecer el sistema.

Una acción correctiva eficaz debe:

Responder oportunamente a la no conformidad.

Controlar y corregir el problema cuando corresponda.

Tratar sus consecuencias.

Determinar las causas.

Comprobar si existen problemas similares en otras áreas.

Implementar las medidas necesarias.

Asignar responsables y plazos.

Verificar la implementación.

Evaluar la eficacia de las medidas adoptadas.

Modificar el Sistema de Gestión Antisoborno cuando sea necesario.

Conservar evidencia documentada del proceso y de sus resultados.

En definitiva, **el objetivo de una acción correctiva no es demostrar que un problema fue cerrado, sino demostrar que la organización aprendió de él y redujo razonablemente la posibilidad de que vuelva a ocurrir**. Este enfoque es coherente con los requisitos actuales de **ISO 37001:2025** para la gestión de no conformidades y acciones correctivas.

6.4. Proceso de certificación por organismos acreditados

Introducción

La **certificación de un Sistema de Gestión Antisoborno según ISO 37001** es un proceso mediante el cual un organismo de certificación independiente evalúa si el sistema implementado por una organización cumple los requisitos establecidos por la norma.

Es importante distinguir entre **ISO y el organismo que certifica**. ISO desarrolla las normas internacionales, pero **ISO no certifica organizaciones ni emite certificados**. La certificación es realizada por organismos externos de certificación.

Cuando se busca una certificación con reconocimiento mediante acreditación, el organismo de certificación debe estar **acreditado por un organismo de acreditación competente para el alcance correspondiente**. La acreditación proporciona una evaluación independiente de la competencia del organismo de certificación.

¿Qué significa certificar ISO 37001?

Certificar ISO 37001 significa que una organización ha sometido su **Sistema de Gestión Antisoborno** a una evaluación realizada por un tercero independiente y que, como resultado del proceso de certificación, se ha determinado que el sistema cumple los requisitos aplicables de la norma.

La certificación se refiere al **sistema de gestión de la organización**, no a que ISO certifique que la organización jamás haya tenido un caso de soborno. Por ello, una certificación no debe interpretarse como una garantía absoluta de que nunca podrá producirse un acto de soborno.

Su finalidad es proporcionar evidencia independiente de que la organización ha establecido e implementado un **sistema de gestión diseñado para prevenir, detectar y responder al soborno**.

Certificación y acreditación son conceptos diferentes

Es fundamental distinguir ambos conceptos.

Certificación: es la evaluación realizada por un organismo de certificación independiente para determinar si el sistema de gestión cumple determinados requisitos.

Acreditación: es el reconocimiento formal de la competencia de un organismo de evaluación de la conformidad para realizar determinadas actividades de evaluación.

Por ejemplo, una organización puede contratar un organismo de certificación para evaluar su Sistema de Gestión Antisoborno.

El organismo de certificación, a su vez, puede estar **acreditado** por un organismo de acreditación competente.

La relación puede entenderse de la siguiente manera:

Organización → organismo de certificación → organismo de acreditación.

La organización busca demostrar la conformidad de su sistema. El organismo de certificación realiza la evaluación. El organismo de acreditación evalúa la competencia e imparcialidad del organismo de certificación dentro de su alcance de acreditación.

¿Quién realiza la certificación?

La certificación de sistemas de gestión es realizada por **organismos de certificación de tercera parte**.

ISO/CASCO identifica la **ISO/IEC 17021-1** como la norma que establece requisitos para los organismos que realizan auditorías y certificación de sistemas de gestión. Entre estos requisitos se encuentran aspectos relacionados con **competencia, imparcialidad, confidencialidad y consistencia**. Esto es importante porque el organismo certificador debe actuar de manera independiente y objetiva.

No debe existir una situación en la que el mismo organismo diseñe el sistema de la organización y después certifique su propio trabajo como si fuera una evaluación independiente.

Selección del organismo de certificación

La organización debe seleccionar cuidadosamente el organismo que realizará la certificación.

Entre los aspectos que puede evaluar se encuentran:

- Experiencia en certificación de sistemas de gestión.
- Competencia de sus auditores.
- Experiencia específica en sistemas antisoborno.
- Alcance de la acreditación.
- Reconocimiento de la acreditación.
- Experiencia en el sector de actividad de la organización.
- Metodología de auditoría.
- Condiciones contractuales.
- Costos y duración del proceso.
- Requisitos de seguimiento y recertificación.

ISO recomienda evaluar diferentes organismos de certificación y comprobar si utilizan las normas pertinentes de evaluación de la conformidad y si están acreditados cuando esto sea un requisito o una condición buscada por la organización.

Preparación antes de solicitar la certificación

Antes de iniciar una auditoría de certificación, la organización debería asegurarse de que su Sistema de Gestión Antisoborno se encuentra **realmente implementado y funcionando**.

No es suficiente con crear documentos.

La organización debe poder demostrar que:

La política antisoborno está establecida.

Los riesgos de soborno han sido evaluados.

Se han implementado controles apropiados.

Se realiza la debida diligencia cuando corresponde.

Los trabajadores conocen sus responsabilidades.

Existen canales para comunicar posibles conductas indebidas.

Los incidentes son tratados e investigados cuando corresponde.

Se realizan auditorías internas.

La dirección revisa el sistema.

Las no conformidades son tratadas mediante acciones correctivas.

Documentación y evidencias

Durante el proceso de certificación, el auditor no se limita a revisar documentos. También busca **evidencias de implementación y funcionamiento**.

Por ejemplo, si la organización afirma que realiza debida diligencia sobre proveedores de alto riesgo, puede ser necesario demostrarlo mediante registros, evaluaciones, aprobaciones y otros documentos pertinentes.

Si afirma que realiza capacitación antisoborno, puede presentar:

- Programas de capacitación.
- Registros de participantes.
- Materiales utilizados.
- Evaluaciones.
- Evidencias de realización.

La diferencia fundamental es:

“Tenemos un procedimiento” no equivale necesariamente a **“el procedimiento funciona y se aplica”.**

Auditoría de certificación

El proceso de certificación incluye una evaluación formal del sistema por parte del organismo de certificación.

En los sistemas de certificación de gestión, ISO/IEC 17021-1 contempla procesos como **auditoría inicial y certificación, actividades de seguimiento y recertificación**, además de procesos para cambios en el alcance, suspensión o retiro de la certificación cuando corresponda. El proceso concreto puede variar según el organismo de certificación y las reglas de acreditación aplicables.

Etapa inicial: revisión de preparación

Antes de la auditoría principal puede realizarse una evaluación inicial de la preparación de la organización.

En esta etapa se puede analizar, entre otros aspectos:

- Información general de la organización.
- Alcance propuesto del sistema.
- Documentación relevante.
- Comprensión de los procesos.
- Nivel de preparación.
- Identificación de posibles áreas problemáticas.

La finalidad es determinar si la organización se encuentra preparada para continuar con la evaluación de certificación.

Auditoría de certificación

La auditoría de certificación busca obtener **evidencia objetiva** sobre el grado de cumplimiento del Sistema de Gestión Antisoborno respecto de los requisitos aplicables.

Los auditores pueden revisar:

- Política antisoborno.
- Evaluación de riesgos.
- Controles financieros.
- Controles comerciales.
- Debida diligencia.
- Gestión de terceros.
- Regalos y hospitalidad.
- Donaciones.
- Capacitación.
- Canales de denuncia.
- Investigación de incidentes.
- Auditorías internas.
- Revisión por la dirección.
- Acciones correctivas.

También pueden realizar entrevistas con trabajadores y responsables de procesos y revisar evidencias relacionadas con la aplicación práctica del sistema.

Evidencia objetiva

Un principio fundamental de la auditoría es trabajar con **evidencia objetiva**. Por ejemplo, si un responsable afirma:

“Todos nuestros proveedores son evaluados antes de ser contratados”.

El auditor puede solicitar evidencias que permitan comprobar esa afirmación.

Puede revisar una muestra de expedientes y comprobar:

- Fecha de evaluación.
- Nivel de riesgo.
- Información analizada.

- Aprobaciones.
- Decisiones adoptadas.
- Fecha de contratación.

De esta forma, la auditoría busca comprobar **cómo funciona realmente el sistema**.

Hallazgos de auditoría

Durante una auditoría pueden identificarse diferentes resultados. Dependiendo de las reglas aplicables al proceso de certificación, pueden existir:

Conformidades: se evidencia el cumplimiento del requisito.

No conformidades: se identifica un incumplimiento de un requisito aplicable.

Observaciones u oportunidades de mejora: pueden utilizarse para señalar aspectos que podrían fortalecerse, según la metodología del organismo certificador.

Las categorías y reglas concretas deben entenderse de acuerdo con el esquema de certificación y los procedimientos del organismo correspondiente.

No conformidades

Si el auditor identifica una **no conformidad**, la organización debe tratarla de acuerdo con el proceso establecido.

Esto puede requerir:

- Analizar la causa.
- Corregir la situación.
- Implementar una acción correctiva.
- Presentar evidencias.
- Verificar la eficacia de la medida.

Una certificación no debería entenderse como un proceso en el que cualquier hallazgo implica automáticamente el fracaso de toda la organización. Lo importante es que las no conformidades sean **tratadas adecuadamente conforme a las reglas de certificación aplicables**.

Decisión de certificación

Una característica importante del proceso es la separación entre **auditoría y decisión de certificación**. El auditor recopila y evalúa evidencias y prepara los resultados correspondientes.

La decisión sobre la certificación debe realizarse conforme a los procedimientos del organismo de certificación y bajo condiciones que protejan la **imparcialidad del proceso**. ISO/IEC 17021-1 establece requisitos específicos para la estructura, recursos y procesos de los organismos de certificación de sistemas de gestión.

Si se determina que los requisitos aplicables han sido satisfechos, el organismo puede emitir el certificado correspondiente.

Emisión del certificado

Cuando la organización supera satisfactoriamente el proceso de certificación, el organismo de certificación emite un **certificado de conformidad**.

El certificado normalmente identifica información como:

- Nombre de la organización.
- Norma respecto de la cual se certifica.
- Alcance de la certificación.
- Identificación del organismo de certificación.
- Condiciones aplicables.
- Fechas relevantes.
- Estado de la certificación.

El **alcance** es especialmente importante.

No debe interpretarse automáticamente que una certificación ISO 37001 cubre absolutamente todas las actividades de una organización. El alcance especifica **qué sistema, actividades, ubicaciones u operaciones están comprendidos**, de acuerdo con el certificado emitido.

La certificación no es permanente sin seguimiento

Obtener el certificado no significa que la organización pueda dejar de gestionar el sistema. Los esquemas de certificación de sistemas de gestión contemplan **actividades de seguimiento y recertificación**.

Por ello, la organización debe continuar:

- Evaluando riesgos.
- Aplicando controles.
- Capacitando al personal.
- Realizando auditorías internas.
- Tratando incidentes.
- Gestionando no conformidades.
- Revisando el sistema.
- Realizando mejoras.

La certificación debe entenderse como parte de un **ciclo continuo de evaluación y mejora**.

Auditorías de seguimiento

Después de la certificación inicial, el organismo certificador realiza actividades de seguimiento de acuerdo con el esquema aplicable. Estas auditorías permiten comprobar que el Sistema de Gestión Antisoborno **continúa implementado y funcionando**.

Durante estas evaluaciones pueden revisarse nuevamente diferentes componentes del sistema, especialmente aquellos relacionados con:

- Cambios importantes.
- Riesgos.
- Resultados de auditorías.
- Incidentes.
- Acciones correctivas.
- Controles.
- Procesos relevantes.

Recertificación

Al finalizar el ciclo de certificación correspondiente, la organización puede someterse a un **proceso de recertificación**.

La finalidad es comprobar nuevamente que el sistema continúa cumpliendo los requisitos aplicables y sigue siendo adecuado para las condiciones actuales de la organización. La recertificación no debe entenderse como una simple renovación administrativa del certificado. Implica una nueva evaluación dentro del esquema correspondiente.

Cambios que pueden afectar la certificación

Durante el período de certificación pueden producirse cambios importantes en la organización.

Por ejemplo:

- Adquisiciones.
- Fusiones.
- Cambios de estructura.
- Nuevas sedes.
- Nuevos países de operación.
- Nuevas actividades.
- Cambios importantes en procesos.
- Modificación del alcance.

Estos cambios pueden requerir comunicación al organismo de certificación y, dependiendo de las circunstancias, una evaluación adicional.

Los organismos de certificación deben contar con procesos para gestionar **cambios que puedan afectar la certificación**, así como para situaciones como ampliación o reducción del alcance, suspensión o retiro de la certificación.

Suspensión o retiro de la certificación

En determinadas circunstancias, una certificación puede ser **suspendida, reducida o retirada** conforme a las reglas aplicables. Esto puede ocurrir, por ejemplo, cuando una

organización deja de cumplir requisitos relevantes o no permite realizar las actividades de seguimiento requeridas.

Por ello, mantener una certificación implica mantener también el **funcionamiento efectivo del sistema**.

Importancia de la acreditación

La acreditación aporta una capa adicional de confianza. El organismo de acreditación evalúa si el organismo de certificación tiene la **competencia, imparcialidad y capacidad necesarias** para realizar sus actividades dentro de su alcance.

ISO explica que la acreditación proporciona una confirmación independiente de la competencia del organismo de certificación. Por ello, cuando una organización busca una certificación acreditada, no debe limitarse a preguntar:

"¿Esta empresa entrega certificados ISO 37001?"

También debe preguntar:

"¿El organismo está acreditado para certificar ISO 37001 dentro del alcance correspondiente?"

Verificación de la certificación

Una certificación acreditada puede ser verificada mediante mecanismos establecidos por el sistema de acreditación y el organismo certificador. ISO señala que los certificados pueden verificarse mediante **IAF CertSearch** u otras fuentes correspondientes al organismo de certificación o al organismo de acreditación. Esto permite que clientes, socios comerciales y otras partes interesadas puedan comprobar la existencia y el estado de determinadas certificaciones.

Certificación y capacitación del personal

Debe mantenerse la diferencia estudiada anteriormente entre:

Certificación de la organización: evalúa el Sistema de Gestión Antisoborno de la organización.

Capacitación del personal: desarrolla conocimientos y competencias de los trabajadores.

Completar un curso de ISO 37001 **no convierte automáticamente a una persona ni a una empresa en "certificada ISO 37001"**.

Del mismo modo, que una empresa obtenga la certificación de su Sistema de Gestión Antisoborno no significa que todos sus trabajadores hayan obtenido una certificación profesional individual. Son conceptos diferentes.

Certificación en el contexto peruano

Para una organización que opera en **Perú**, resulta especialmente importante verificar que el organismo de certificación seleccionado tenga el **alcance de acreditación apropiado** y que el certificado pueda ser comprobado mediante las fuentes correspondientes.

La organización también debe revisar cualquier requisito contractual, sectorial o regulatorio que pueda exigir una determinada forma de acreditación o reconocimiento.

Esto es especialmente relevante para empresas que participan en **contrataciones, proyectos con entidades públicas, minería, construcción o relaciones comerciales con grandes empresas**, donde determinados clientes pueden establecer requisitos específicos de cumplimiento.

Ejemplo práctico

Una empresa peruana decide implementar ISO 37001.

Primero desarrolla su Sistema de Gestión Antisoborno:

Evalúa los riesgos.

Establece una política antisoborno.

Implementa controles.

Realiza debida diligencia.

Capacita al personal.

Establece canales de denuncia.

Realiza una auditoría interna.

Ejecuta la revisión por la dirección.

Trata las no conformidades mediante acciones correctivas.

Después selecciona un organismo de certificación con el alcance correspondiente. El organismo realiza la evaluación. Durante la auditoría identifica algunas no conformidades. La empresa analiza sus causas y aplica acciones correctivas. El organismo revisa las evidencias correspondientes conforme a sus procedimientos. Finalmente, si se cumplen las condiciones establecidas, se toma la decisión de certificación y se emite el certificado.

A partir de ese momento, la organización debe **mantener y mejorar el sistema**, además de someterse a las actividades de seguimiento y recertificación correspondientes.

Errores frecuentes

Uno de los errores más comunes es pensar que **“tener documentos ISO” equivale a estar certificado**.

No es así.

Otro error es creer que **ISO entrega directamente los certificados**.

ISO no realiza certificaciones.

También es incorrecto afirmar que cualquier empresa que venda servicios de consultoría puede automáticamente **certificar** el sistema que ayudó a implementar.

La certificación de tercera parte requiere un proceso independiente y sujeto a requisitos de evaluación de la conformidad.

Idea clave

El proceso de certificación de ISO 37001 debe entenderse como una **evaluación independiente del Sistema de Gestión Antisoborno**.

El proceso puede resumirse de forma general:

Implementación del sistema → preparación → selección del organismo de certificación → auditoría → tratamiento de hallazgos → decisión de certificación → emisión del certificado → seguimiento → recertificación.

La organización debe recordar que:

ISO desarrolla la norma, pero no certifica organizaciones.

El organismo de certificación realiza la auditoría y certificación.

La acreditación reconoce formalmente la competencia del organismo de certificación dentro de un alcance determinado.

La certificación se refiere al sistema de gestión y a su alcance definido.

La certificación requiere mantenimiento y seguimiento.

La certificación no constituye una garantía absoluta de ausencia de soborno.

En definitiva, una certificación ISO 37001 representa una **evaluación independiente de la conformidad del Sistema de Gestión Antisoborno con los requisitos aplicables**, proporcionando a la organización y a sus partes interesadas una evidencia adicional de que existe un sistema estructurado para gestionar los riesgos relacionados con el soborno.

Este curso ha sido desarrollado por **INFOSET** con el objetivo de proporcionar a los trabajadores, técnicos y profesionales las **competencias fundamentales en materia de prevención del soborno, cumplimiento y gestión antisoborno**, necesarias para desenvolverse de manera responsable y ética en organizaciones públicas y privadas en el Perú.

Creemos firmemente que la **cultura de integridad y prevención del soborno** no es solo una obligación normativa, sino una **necesidad estratégica** para las organizaciones que desean proteger su reputación, fortalecer sus procesos y desarrollar relaciones comerciales y profesionales basadas en la transparencia y la confianza.

Este curso busca **acercar los principios de ISO 37001 y del cumplimiento antisoborno** a la realidad cotidiana de los trabajadores y profesionales. A través de un lenguaje claro y práctico, se abordan conceptos relacionados con el soborno, el marco normativo peruano e internacional, la evaluación de riesgos, la debida diligencia, los controles financieros y comerciales, los canales de denuncia, las investigaciones y la mejora continua.

Es fundamental que los participantes **comprendan y apliquen lo aprendido en sus funciones cotidianas**, contribuyendo a prevenir situaciones de soborno y fortaleciendo una cultura organizacional basada en la integridad. Un sistema de gestión antisoborno eficaz requiere no solo políticas y procedimientos, sino también **personas capacitadas, responsables y comprometidas con el cumplimiento**.

La difusión de este contenido está **permitida siempre que se mantenga el reconocimiento a INFOSET** como entidad autora. Compartir este conocimiento forma parte de nuestra misión: **democratizar el acceso a la capacitación profesional y promover una cultura de integridad**, especialmente entre trabajadores y organizaciones que buscan fortalecer sus conocimientos en materia de cumplimiento.

Agradecemos a cada participante por su interés, tiempo y compromiso con su desarrollo profesional. Con cada persona que comprende mejor los riesgos de soborno y aprende a prevenirlos, **las organizaciones peruanas avanzan hacia una gestión más transparente, responsable y sostenible**.

Administración de INFOSET