WHITEPAPER TÉCNICO

Claves de la ISO 37003

Sistemas de Gestión del Control del Fraude

Síntesis normativa y divulgativa de la primera norma internacional dedicada al control del fraude

DOCUMENTO	Whitepaper técnico — Claves de la ISO 37003: Sistemas de Gestión del Control del Fraude
NORMA	ISO 37003:2025 — Sistemas de gestión del control del fraude. Orientación para organizaciones que gestionan el riesgo de fraude
PUBLICACIÓN	29 de mayo de 2025 · Primera edición · 45 páginas · Comité Técnico ISO/TC 309
TIPO DE NORMA	Tipo B — orientación. No contiene requisitos certificables equivalentes a ISO 37001 o ISO 37301
ELABORADO POR	Lic. Luis María González Vicente, MBA — Representante Legal, theDUEco. S.R.L.
CONTACTO	Cel. +591 77299739 · luismariagonzalez@thedueco.bo
VERSIÓN	1.0 — Agosto de 2026
CARÁCTER	**Documento divulgativo de acceso público. Citable con atribución a theDUEco. S.R.L.**

Nota editorial. Este documento es una síntesis normativa y divulgativa de la ISO 37003:2025. No sustituye la compra ni la lectura de la norma oficial. El texto siguiente no reproduce literalmente la norma ISO, sino que la explica y adapta a un formato de whitepaper.

Consultas sobre este documento: Lic. Luis María González Vicente, MBA — Representante Legal, theDUEco. S.R.L. · Cel. +591 77299739 · luismariagonzalez@thedueco.bo

> *Su propósito no es garantizar que nunca se producirá fraude, sino aumentar la capacidad de la organización para prevenirlo, detectarlo, responder, recuperar pérdidas y aprender de los incidentes.*

Contenido

01 Introducción

El fraude constituye uno de los riesgos más complejos para las organizaciones. Puede provocar pérdidas económicas, responsabilidades legales, interrupciones operativas, afectación a clientes y terceros, deterioro reputacional y pérdida de confianza. Además, su evolución tecnológica ha multiplicado las formas mediante las cuales una organización puede ser atacada o utilizada para cometer actos deshonestos.

Frente a este escenario, las políticas aisladas, los controles financieros tradicionales y las investigaciones reactivas ya no resultan suficientes. La organización necesita un enfoque integral que articule gobierno, cultura, evaluación de riesgos, controles internos, tecnología, canales de reporte, investigación y mejora continua.

La ISO 37003:2025, Sistemas de gestión del control del fraude — Orientación para organizaciones que gestionan el riesgo de fraude, ofrece ese marco. Publicada en mayo de 2025 por el Comité Técnico ISO/TC 309, constituye la primera norma internacional dedicada específicamente al establecimiento, implementación, evaluación, mantenimiento y mejora de un Sistema de Gestión del Control del Fraude o **Fraud Control Management System — FCMS**. Es aplicable a organizaciones públicas, privadas y sin fines de lucro, cualquiera sea su tamaño, estructura o actividad.

La norma entiende el fraude, en términos generales, como una conducta intencionalmente deshonesta que produce o puede producir una ganancia o pérdida y generar daño económico o social. El concepto abarca la falsificación, ocultamiento o destrucción de documentación; el uso indebido de información, activos o posiciones; la manipulación de datos; el engaño; la apropiación de recursos y otras conductas equivalentes. Una conducta fraudulenta no necesita coincidir siempre con un delito tipificado para representar un riesgo que deba ser gestionado.

ISO 37003 comprende:

- Fraude interno cometido contra la organización.
- Fraude externo cometido por clientes, proveedores, ciberdelincuentes u otros terceros.
- Colusión entre personal interno y actores externos.
- Fraude cometido por la propia organización.
- Fraude realizado por agentes, representantes o socios en nombre o beneficio de la organización.
- Fraude facilitado por tecnologías digitales, automatización o inteligencia artificial.

Su propósito no es garantizar que nunca se producirá fraude, sino aumentar la capacidad de la organización para prevenirlo, detectarlo, responder, recuperar pérdidas y aprender de los incidentes.

Una precisión importante. ISO 37003 es una norma de orientación Tipo B. No contiene requisitos de certificación equivalentes a los de ISO 37001 o ISO 37301. Por ello, una organización puede implementar sus recomendaciones y someter el sistema a auditorías o evaluaciones independientes, pero debe ser prudente al afirmar que está "certificada" conforme a ISO 37003.

Este whitepaper explica sus fundamentos, estructura, principales recomendaciones y el proceso práctico para convertirlas en un sistema eficaz.

02 Estructura de la ISO 37003

La ISO 37003 se organiza en los siguientes capítulos:

CAP.	TÍTULO	CAP.	TÍTULO
1	Alcance	6	Planificación

CAP.	TÍTULO	CAP.	TÍTULO
2	Referencias normativas	7	Apoyo
3	Términos y definiciones	8	Operación
4	Contexto de la organización	9	Evaluación del desempeño
5	Liderazgo	10	Mejora

La norma incluye también:

- **Anexo A:** ejemplos de riesgos de fraude que afectan a entidades globales.
- **Anexo B:** modelos y orientaciones para la prevención del fraude.

Aunque los capítulos 4 a 10 presentan la arquitectura habitual de un sistema de gestión, el elemento distintivo de ISO 37003 se encuentra en su capítulo 8, que desarrolla el ciclo operativo completo:

> *Prevenir el fraude, detectarlo cuando los controles preventivos son superados y responder de forma rápida, proporcionada y documentada.*

03 La importancia del control del fraude en las organizaciones

El fraude es una conducta deliberada. A diferencia del error, supone intención de engañar, ocultar, manipular o aprovechar indebidamente información, activos, procesos o posiciones de confianza.

Puede manifestarse en cualquier nivel de una organización y adoptar formas muy diferentes:

- Apropiación de efectivo, inventarios o equipos.
- Facturación falsa o duplicada.
- Proveedores ficticios o vinculados a empleados.
- Manipulación de estados financieros o indicadores.
- Gastos y reembolsos inexistentes.
- Alteración de procesos de selección o contratación.
- Uso indebido de información privilegiada.
- Fraude fiscal, de seguros, subvenciones o ayudas.
- Suplantación de identidad.
- Manipulación de pagos y datos bancarios.
- Ciberfraude, ransomware o fraude mediante ingeniería social.
- Acuerdos colusorios y manipulación de mercados.
- Fraude cometido contra clientes o autoridades en nombre de la organización.

El impacto no se limita a la pérdida financiera inmediata. Un incidente puede provocar investigaciones regulatorias, litigios, sanciones contractuales, suspensión de operaciones, pérdida de licencias, deterioro de relaciones comerciales, afectación de víctimas y pérdida de confianza interna.

Por qué los controles tradicionales no son suficientes

Muchas organizaciones cuentan con auditoría financiera, controles de autorización o un canal de denuncias, pero estos mecanismos suelen funcionar de manera fragmentada.

Un sistema eficaz requiere responder, entre otras, a las siguientes preguntas:

- ¿Qué modalidades de fraude pueden afectar a cada proceso?
- ¿Quién podría cometerlas y con qué motivación?
- ¿Qué activos, sistemas o terceros podrían ser utilizados?
- ¿Qué controles existen y cómo podrían ser eludidos?
- ¿Qué señales permitirían descubrir el fraude?
- ¿Quién recibe, evalúa y escala una sospecha?
- ¿Cómo se preserva la evidencia digital?
- ¿Quién investiga y quién decide una sanción?
- ¿Cómo se recuperan activos o fondos?
- ¿Cómo se evita que el fraude vuelva a ocurrir?

ISO 37003 organiza estas preguntas dentro de un sistema permanente de gobierno y gestión.

Beneficios de un Sistema de Gestión del Control del Fraude

Entre los principales beneficios se encuentran:

- Reducción de la exposición a pérdidas económicas.
- Mayor protección de activos, datos y recursos.
- Fortalecimiento del ambiente de control interno.
- Detección más temprana de anomalías.
- Claridad en funciones, responsabilidades y escalamiento.
- Mayor calidad y objetividad de las investigaciones.
- Mejor capacidad para recuperar fondos o bienes.
- Protección de clientes, trabajadores y demás interesados.
- Mayor confianza de inversores, financiadores y socios.
- Mejor preparación ante revisiones regulatorias.
- Integración entre cumplimiento, riesgos, auditoría, finanzas, recursos humanos, seguridad y tecnología.
- Aprendizaje sistemático a partir de incidentes.

ISO advierte que ningún sistema puede eliminar completamente el fraude. Su valor consiste en fortalecer la resiliencia y la capacidad de anticipación y respuesta.

04 El origen y las novedades de la ISO 37003

A diferencia de otras normas que sustituyen o actualizan estándares anteriores, ISO 37003 no reemplaza directamente a una norma ISO específica sobre fraude. Surge para cubrir una brecha: la ausencia de una referencia internacional que integrara prevención, detección, investigación, respuesta, recuperación y mejora en un único sistema.

El proyecto fue aprobado en 2022, pasó por las etapas de borrador de comité, consulta internacional y aprobación final, y fue publicado el 29 de mayo de 2025. La primera edición tiene 45 páginas.

De los controles aislados a un sistema integral

Antes de ISO 37003, muchas organizaciones gestionaban el fraude mediante instrumentos separados:

- Código de ética.

- Matriz de riesgos.
- Controles contables.
- Auditoría interna.
- Canal de denuncias.
- Investigaciones laborales.
- Ciberseguridad.
- Debida diligencia de terceros.
- Procedimientos disciplinarios.
- Pólizas de seguro.

El problema no era necesariamente la ausencia de controles, sino la falta de coordinación, responsabilidades claras y aprendizaje común.

ISO 37003 propone convertir esas herramientas en un Fraud Control Management System. Esto significa que las medidas antifraude deben:

- Partir del contexto y de una evaluación específica del riesgo.
- Responder a objetivos definidos.
- Contar con liderazgo y recursos.
- Integrarse en los procesos ordinarios.
- Ser documentadas y monitoreadas.
- Someterse a auditoría y revisión.
- Actualizarse a partir de resultados e incidentes.

Principales novedades

Alcance amplio del fraude. La norma no se limita al fraude de empleados contra la empresa. Incluye fraude interno, externo, colusorio y fraude cometido por la propia organización o por quienes actúan en su nombre.

Atención a incentivos y metas. ISO 37003 reconoce que determinados objetivos de ventas, producción, rentabilidad o reducción de costos pueden crear presiones indebidas. Por ello, recomienda revisar los sistemas de remuneración y las metas basadas en desempeño para evitar que incentiven la manipulación o el ocultamiento.

Pruebas de presión de controles. No basta con documentar que existe un control. La organización debería comprobar si puede ser vulnerado, eludido o neutralizado. Las pruebas de presión, simulaciones y ejercicios de fraude permiten detectar debilidades antes de que sean explotadas.

Coordinación con seguridad de la información. El fraude moderno suele involucrar sistemas, credenciales, datos personales, dispositivos y evidencias digitales. La norma asigna relevancia expresa a la función de seguridad de la información.

Inteligencia artificial. ISO 37003 incorpora la utilización de sistemas de inteligencia artificial dentro de los mecanismos de detección. Sin embargo, su uso debe contar con datos adecuados, supervisión, criterios de escalamiento y revisión humana, evitando confiar de manera automática en los resultados de un algoritmo.

Respuesta detallada. La norma presta especial atención a la fase posterior al descubrimiento del fraude: contención, evidencia digital, investigación, decisiones disciplinarias, gestión de crisis, comunicación, recuperación de activos y revisión de controles.

05 Relación de la ISO 37003 con otras normas y marcos

ISO 37003 puede funcionar de forma independiente, pero alcanza mayor eficacia cuando se integra con otros sistemas de gobierno, riesgo, cumplimiento y seguridad.

ISO 37000: Gobernanza de las organizaciones

ISO 37000 aporta principios generales de gobernanza. ISO 37003 desarrolla esos principios en el ámbito específico del fraude, reforzando la responsabilidad del órgano de gobierno, la supervisión y la rendición de cuentas.

ISO 31000: Gestión de riesgos

ISO 31000 proporciona principios y un proceso general para identificar, analizar, valorar y tratar riesgos. ISO 37003 aplica esa lógica al riesgo de fraude, incorporando escenarios, perpetradores, métodos, señales de alerta, controles y riesgo residual.

ISO 37001: Sistemas de gestión antisoborno

El soborno puede formar parte de un esquema fraudulento, pero ambas normas tienen alcances diferentes:

ISO 37001	ISO 37003
Se concentra específicamente en el soborno.	Aborda el universo más amplio del fraude.
Es Tipo A y contiene requisitos certificables.	Es Tipo B y proporciona orientación.

Una organización puede integrar ambas bajo una política común de integridad, compartiendo evaluación de riesgos, debida diligencia, capacitación, controles, canales de reporte, investigaciones y auditorías. La edición vigente de ISO 37001 también fue actualizada en 2025.

ISO 37002: Sistemas de gestión de denuncias

ISO 37002 orienta sobre la recepción, evaluación, tratamiento y cierre de reportes. Es un complemento directo de ISO 37003 porque muchos fraudes se descubren mediante alertas de empleados, clientes, proveedores u otros interesados.

El canal debe inspirar confianza, preservar la confidencialidad, proteger frente a represalias y permitir un tratamiento imparcial.

ISO/TS 37008: Investigaciones internas

ISO/TS 37008 ofrece orientación para planificar y realizar investigaciones internas. Complementa el capítulo de respuesta de ISO 37003 en aspectos como:

- Mandato de investigación.
- Independencia y competencia del investigador.
- Planificación del caso.

- Obtención y preservación de evidencia.
- Entrevistas.
- Confidencialidad.
- Informes y decisiones posteriores.

ISO 37009: Conflictos de intereses

Los conflictos de intereses pueden crear oportunidades para favoritismo, colusión, desviación de decisiones o fraude. ISO 37009 proporciona una referencia complementaria para identificarlos, declararlos, evaluarlos y tratarlos.

ISO 37301: Sistemas de gestión de Compliance

ISO 37301 cubre el conjunto de obligaciones de cumplimiento de la organización. ISO 37003 profundiza en un riesgo particular: el fraude.

Un sistema integrado puede compartir:

- Análisis del contexto.
- Identificación de interesados.
- Política y responsabilidades.
- Evaluación de riesgos.
- Formación.
- Documentación.
- Canal de denuncias.
- Auditorías.
- Revisión por la dirección.
- Acciones correctivas.

ISO reconoce expresamente que ISO 37003 complementa a ISO 37001 e ISO 37301 para fortalecer la integridad y la gestión de riesgos.

ISO/IEC 27001: Seguridad de la información

La relación es especialmente importante para:

- Controles de acceso.
- Segregación de privilegios.
- Registros de auditoría.
- Protección de datos.
- Gestión de identidades.
- Monitoreo de eventos.
- Respuesta a incidentes.
- Conservación de evidencia digital.
- Fraude basado en suplantación o manipulación de sistemas.

ISO 22301: Continuidad del negocio

Un fraude de gran magnitud puede generar una crisis operativa. ISO 22301 ayuda a preparar la continuidad y recuperación de actividades críticas.

COSO y ACFE

Aunque no son normas ISO, sus marcos de control interno y gestión del riesgo de fraude son complementarios. Pueden ayudar a diseñar controles, evaluar el ambiente organizacional y estructurar escenarios de fraude.

06 Estructura y ciclo de trabajo de la ISO 37003

Capítulo 1. Alcance

Define la finalidad y aplicabilidad del documento. ISO 37003 está dirigida a organizaciones de cualquier tamaño y sector.

No está concebida como una guía para que consumidores individuales gestionen fraudes personales. Su unidad de aplicación es la organización o una parte definida de ella.

Capítulo 2. Referencias normativas

La norma no contiene referencias normativas obligatorias. Puede aplicarse por sí misma, aunque recomienda o cita otras fuentes como apoyo.

Capítulo 3. Términos y definiciones

Establece el vocabulario necesario para interpretar la orientación. Entre los conceptos relevantes se encuentran:

- Fraude.
- Organización.
- Órgano de gobierno.
- Alta dirección.
- Personal.
- Socio de negocio.
- Riesgo de fraude.
- Control del fraude.
- Sistema de Gestión del Control del Fraude.
- Información documentada.
- Auditoría.
- No conformidad.
- Acción correctiva.

Capítulo 4. Contexto de la organización

La organización debe comprender los factores internos y externos que afectan su exposición al fraude.

FACTORES EXTERNOS	FACTORES INTERNOS
— Legislación y regulación. — Mercado y competencia. — Condiciones económicas. — Desarrollo tecnológico. — Tipologías delictivas. — Cadenas de suministro. — Jurisdicciones de operación. — Expectativas de autoridades, clientes y financiadores.	— Modelo de negocio. — Estructura societaria. — Cultura y conducta de liderazgo. — Sistemas de remuneración. — Procesos de contratación y pago. — Uso de efectivo y activos físicos. — Sistemas de información. — Dependencia de terceros. — Historial de incidentes. — Recursos y competencias antifraude.

La organización debe identificar interesados, determinar el alcance del FCMS, establecer sus procesos y realizar una evaluación del riesgo de fraude.

Capítulo 5. Liderazgo

El órgano de gobierno y la alta dirección deben demostrar compromiso con el control del fraude.

La orientación comprende:

- Supervisión del FCMS.
- Política de control del fraude.
- Integración con los procesos de la organización.
- Asignación de recursos.
- Promoción de una cultura de integridad.
- Definición de funciones y autoridades.
- Delegación controlada de decisiones.
- Establecimiento de una función de control del fraude.
- Coordinación con seguridad de la información y auditoría interna.

> *El principio esencial es que el riesgo de fraude pertenece a la dirección y a los responsables de los procesos. Auditoría interna puede evaluar el sistema, pero no sustituye la responsabilidad de gestionarlo.*

Capítulo 6. Planificación

La organización debe determinar cómo tratará los riesgos y oportunidades relacionados con el FCMS.

La planificación incluye:

- Priorización de riesgos.
- Definición de objetivos antifraude.
- Responsables.
- Recursos.
- Plazos.
- Indicadores.
- Criterios de evaluación.
- Planificación de cambios.

Los objetivos deben ser coherentes con la política, medibles cuando sea posible y actualizados ante cambios en procesos, tecnologías, mercados o terceros.

Capítulo 7. Apoyo

El sistema necesita recursos humanos, financieros y tecnológicos suficientes.

La orientación comprende:

- Competencias del personal.
- Procesos de selección y empleo.
- Formación y concientización.
- Capacitación de socios de negocio cuando sea pertinente.
- Comunicación interna y externa.
- Creación y actualización de documentos.
- Control de la información documentada.
- Conservación de registros.

— Confidencialidad.
— Protección de información sensible.

La formación debe adaptarse al riesgo. Un trabajador de almacén, un administrador de sistemas, un comprador y un alto directivo no enfrentan los mismos escenarios ni necesitan idéntico contenido.

Capítulo 8. Operación

Es el núcleo de la norma y se divide en planificación operativa, prevención, detección y respuesta.

PREVENCIÓN DEL FRAUDE	DETECCIÓN DEL FRAUDE	RESPUESTA FRENTE AL FRAUDE
— Desarrollo de un marco de integridad. — Gestión de conflictos de intereses. — Controles internos. — Ambiente de control. — Pruebas de presión. — Metas basadas en desempeño. — Verificación de personal. — Evaluación y gestión de socios de negocio. — Fraude facilitado por tecnología. — Seguridad física y gestión de activos.	— Revisión posterior de transacciones. — Análisis de informes contables y gerenciales. — Identificación de señales de alerta. — Analítica de datos. — Reporte de sospechas. — Sistemas de inteligencia artificial. — Gestión de quejas. — Entrevistas de salida.	— Actuaciones inmediatas. — Contención del daño. — Primera respuesta ante evidencia digital. — Investigación. — Evaluación objetiva de denuncias y agravios. — Procedimientos disciplinarios. — Separación entre investigación y decisión. — Gestión de crisis. — Reporte y escalamiento interno. — Registro de eventos. — Análisis y presentación de informes. — Comunicaciones o reportes externos. — Recuperación de fondos o bienes. — Respuesta ante incidentes relacionados con socios. — Seguros contra fraude. — Revisión de controles después del incidente. — Evaluación del impacto sobre interesados. — Interrupción de esquemas fraudulentos.

Capítulo 9. Evaluación del desempeño

La organización debe evaluar la pertinencia, adecuación y eficacia del sistema mediante:

— Monitoreo.
— Indicadores.
— Análisis de tendencias.
— Auditorías internas.
— Auditorías externas.
— Revisión por la dirección.
— Seguimiento de resultados.

La inclusión de una auditoría externa no convierte a ISO 37003 en una norma certificable. Una auditoría independiente puede evaluar diseño, implementación, funcionamiento o madurez, pero la norma sigue siendo de orientación.

Capítulo 10. Mejora

La organización debe aprender de las deficiencias e incidentes mediante:

- Corrección inmediata.
- Investigación de causas.
- Acción correctiva.
- Revisión de eficacia.
- Actualización de riesgos.
- Rediseño de controles.
- Mejora continua.

Ciclo de trabajo

1. PLANIFICAR — CAP. 4, 5 Y 6	2. HACER — CAP. 7 Y 8	3. VERIFICAR — CAP. 9	4. ACTUAR — CAP. 10
— Entender el contexto. — Definir el alcance. — Evaluar riesgos. — Aprobar la política. — Asignar responsabilidades. — Establecer objetivos. — Planificar controles.	— Asignar recursos. — Formar al personal. — Comunicar. — Documentar. — Aplicar controles preventivos. — Implementar mecanismos de detección. — Preparar la respuesta.	— Medir resultados. — Analizar incidentes. — Auditar. — Revisar el sistema por la dirección.	— Corregir debilidades. — Tratar causas raíz. — Actualizar controles. — Mejorar continuamente.

07 Las 7 claves de la ISO 37003

1. Contexto y evaluación del riesgo de fraude

El punto de partida es comprender cómo puede producirse el fraude en la realidad particular de la organización.

La evaluación debe considerar:

- Procesos y ubicaciones.
- Productos y servicios.
- Personas y cargos.
- Activos e información.
- Sistemas tecnológicos.
- Terceros.
- Incentivos y presiones.
- Métodos de ocultamiento.
- Controles existentes.

— Daños potenciales.

No se trata de crear una lista genérica de delitos, sino de formular escenarios concretos. Por ejemplo:

> *Un empleado con acceso al maestro de proveedores crea o modifica una cuenta bancaria, introduce facturas ficticias y dirige el pago hacia una cuenta controlada por él o por un colaborador.*

Ese escenario permite identificar actores, método, activos, controles y señales de alerta.

2. Liderazgo, integridad y supervisión

La alta dirección debe establecer un mensaje inequívoco: el fraude no es aceptable aunque produzca resultados comerciales favorables.

El liderazgo debe expresarse mediante decisiones:

— Aprobar la política.
— Asignar presupuesto.
— Exigir rendición de cuentas.
— Proteger a quienes reportan de buena fe.
— Evitar interferencias en investigaciones.
— Aplicar medidas consistentes.
— Revisar los resultados del sistema.
— Corregir incentivos perjudiciales.

La cultura se demuestra mediante la coherencia entre lo que se declara y lo que se premia, tolera o sanciona.

3. Funciones y responsabilidades claras

La organización debe definir quién:

— Supervisa el sistema.
— Realiza la evaluación de riesgos.
— Diseña controles.
— Opera los controles.
— Monitorea transacciones.
— Recibe alertas.
— Decide el inicio de una investigación.
— Investiga.
— Adopta decisiones disciplinarias.
— Autoriza comunicaciones externas.
— Informa al órgano de gobierno.

La separación entre investigación y decisión protege la imparcialidad y reduce conflictos de intereses.

4. Personas, terceros, formación y documentación

El control del fraude depende de personas competentes y de información confiable.

INTEGRAR EL RIESGO DE FRAUDE EN	MEDIDAS PROPORCIONALES SOBRE TERCEROS
— Selección y contratación. — Promoción y movilidad. — Acceso a funciones sensibles. — Declaraciones de integridad. — Conflictos de intereses. — Evaluación de desempeño. — Formación. — Procesos de salida.	— Identificación y verificación. — Beneficiario final. — Reputación. — Conflictos y vinculaciones. — Capacidad real. — Condiciones de pago. — Cláusulas contractuales. — Monitoreo. — Derecho de auditoría. — Reacción frente a incumplimientos.

5. Prevención, detección y respuesta

Las tres funciones son inseparables.

— **La prevención** reduce la oportunidad.
— **La detección** permite descubrir lo que supera la prevención.
— **La respuesta** contiene el daño, esclarece hechos, recupera activos y evita la repetición.

> *Un sistema centrado únicamente en prevención puede generar una falsa sensación de seguridad. Un sistema basado solo en investigaciones siempre llegará tarde.*

6. Evaluación del desempeño

La organización necesita indicadores que permitan evaluar si el sistema funciona.

Algunos ejemplos son:

— Porcentaje de riesgos con controles asignados.
— Controles probados y controles deficientes.
— Cobertura de debida diligencia.
— Alertas generadas por analítica.
— Tiempo entre alerta y evaluación.
— Tiempo de investigación.
— Pérdidas por fraude.
— Fondos recuperados.
— Reincidencia.
— Acciones correctivas vencidas.
— Percepción de confianza en el canal de reporte.
— Cobertura y eficacia de la formación.

La ausencia de denuncias no demuestra necesariamente ausencia de fraude. Puede indicar desconocimiento, miedo o falta de confianza.

7. Mejora continua

Cada incidente debe convertirse en una fuente de aprendizaje.

Después de un fraude, la organización debe preguntarse:

- ¿Qué control falló?
- ¿El control estaba mal diseñado o no se ejecutó?
- ¿Hubo colusión?
- ¿Se anularon alertas?
- ¿Existieron presiones comerciales?
- ¿Se ignoraron antecedentes?
- ¿La información no llegó al nivel adecuado?
- ¿El mismo esquema puede existir en otras áreas?
- ¿Qué cambios son necesarios?

La acción correctiva debe tratar la causa, no limitarse a sancionar al perpetrador.

08 Cómo implementar un Sistema de Gestión del Control del Fraude

01 — **Obtener compromiso formal.** La implementación debe comenzar con una decisión del órgano de gobierno o la alta dirección. Se recomienda formalizar:

— Mandato del proyecto. — Patrocinador ejecutivo. — Responsable del FCMS. — Equipo interdisciplinario.	— Recursos. — Calendario. — Mecanismos de reporte.

02 — **Definir el alcance.** El alcance puede abarcar toda la organización o una parte claramente delimitada. Debe especificar:

— Entidades jurídicas. — Unidades. — Países. — Procesos.	— Productos. — Sistemas. — Terceros relevantes. — Interfaces con otros sistemas.

Un alcance demasiado limitado puede dejar fuera procesos donde el fraude se origina o materializa.

03 — **Analizar el contexto.** Se recopila información sobre:

— Modelo de negocio. — Estructura. — Entorno regulatorio. — Volumen de transacciones. — Uso de tecnología. — Personal.	— Terceros. — Historial de incidentes. — Evaluaciones previas. — Auditorías. — Quejas. — Cultura.

04 — **Realizar la evaluación del riesgo de fraude.** Se desarrollan escenarios mediante entrevistas, talleres, análisis de datos, revisión documental e información externa. Para cada escenario se determina:

— Evento. — Actor. — Método. — Activo afectado. — Causas y condiciones. — Probabilidad. — Impacto.	— Controles existentes. — Eficacia de controles. — Riesgo residual. — Tratamiento. — Responsable. — Indicadores de alerta.

05 — Realizar un análisis de brechas. Se compara la situación actual con la orientación de ISO 37003. El análisis debe identificar:

— Elementos existentes. — Elementos parciales. — Ausencias. — Duplicidades.	— Responsabilidades confusas. — Controles no probados. — Documentos desactualizados. — Necesidades de integración.

06 — Aprobar política, objetivos y gobierno. La política debería incluir:

— Prohibición del fraude. — Alcance. — Compromiso de investigar. — Protección de reportantes. — Consecuencias.	— Cooperación con autoridades. — Recuperación de activos. — Responsabilidades. — Mejora continua.

Los objetivos deben derivar de la evaluación de riesgos.

07 — Diseñar y fortalecer controles preventivos. Entre los controles posibles:

— Segregación de funciones. — Doble autorización. — Restricciones de acceso. — Conciliaciones. — Confirmaciones independientes. — Rotación en puestos sensibles. — Vacaciones obligatorias. — Control de cambios en proveedores.	— Verificación de cuentas bancarias. — Debida diligencia. — Gestión de conflictos. — Inventarios. — Controles físicos. — Protección de datos. — Pruebas de presión. — Revisión de metas e incentivos.

08 — Implementar mecanismos de detección. El programa puede combinar:

— Canal confidencial. — Monitoreo de transacciones. — Reglas automatizadas. — Analítica de datos. — Inteligencia artificial. — Revisión de excepciones.	— Control continuo. — Quejas de clientes. — Información de terceros. — Entrevistas de salida. — Auditorías temáticas.

Toda alerta necesita criterios de evaluación y escalamiento.

09 — Preparar el plan de respuesta. El plan debe establecer:

— Equipo de respuesta.	— Comunicación interna y externa.

— Autoridad para ordenar medidas urgentes. — Preservación de evidencia. — Criterios para investigar. — Independencia. — Privacidad y confidencialidad. — Relación con asesoría jurídica.	— Notificación a autoridades. — Gestión de crisis. — Recuperación. — Seguro. — Atención a víctimas e interesados. — Cierre y aprendizaje.

10 — Formar y comunicar. La formación general debería explicar:

— Qué se considera fraude. — Cómo reconocer señales. — Cómo reportar.	— Protección disponible. — Consecuencias. — Responsabilidad individual.

La formación especializada debe dirigirse a compras, finanzas, ventas, tecnología, recursos humanos, auditoría, seguridad y dirección.

11 — Medir, auditar y revisar. El sistema debe contar con:

— Indicadores. — Informes periódicos. — Auditorías internas.	— Evaluaciones externas cuando sean útiles. — Revisión formal por la dirección. — Seguimiento de acciones.

12 — Mejorar continuamente. Los cambios pueden originarse en:

— Incidentes. — Auditorías. — Nuevas tecnologías. — Cambios regulatorios. — Nuevos productos.	— Adquisiciones. — Entrada en otros países. — Nuevos proveedores. — Modificaciones en el modelo de negocio.

Documentos y evidencias recomendables

Una implementación madura debería producir:

GOBIERNO Y RIESGO	OPERACIÓN Y EVIDENCIA
— Política de control del fraude. — Alcance del FCMS. — Mapa de procesos. — Registro de riesgos de fraude. — Matriz de controles. — Plan de tratamiento. — Organigrama de responsabilidades. — Procedimiento de conflictos de intereses. — Programa de debida diligencia.	— Procedimiento de reporte. — Plan de respuesta. — Protocolo de evidencia digital. — Procedimiento de investigación. — Registro de eventos. — Registro de pérdidas y recuperaciones. — Programa de formación. — Indicadores. — Informes de auditoría. — Actas de revisión de dirección. — Registro de acciones correctivas.

09 La importancia del mapa de riesgos de fraude

El mapa de riesgos permite representar de manera ordenada los escenarios de fraude, su exposición y las prioridades de tratamiento.

> *No debe confundirse con una lista genérica de delitos. Un riesgo de fraude debe expresar cómo podría suceder.*

Elementos del mapa

ELEMENTO	CONTENIDO
Identificador	Código que permita seguir el riesgo.
Proceso	Área donde puede producirse: compras, ventas, tesorería, inventario, nómina, tecnología, impuestos o subvenciones.
Escenario	Descripción de la modalidad de fraude.
Actor	Empleado, directivo, proveedor, cliente, agente, ciberdelincuente o combinación de actores.
Método	Forma de ejecución: falsificación, colusión, manipulación de datos, suplantación, abuso de acceso o facturación ficticia.
Activo o interesado afectado	Dinero, inventario, datos, propiedad intelectual, clientes, autoridades o reputación.
Causas	Presión, oportunidad, conflictos, controles deficientes o privilegios excesivos.
Controles existentes	Medidas preventivas y detectivas.
Riesgo inherente	Nivel previo a considerar controles.
Eficacia del control	Evaluación de diseño y funcionamiento.
Riesgo residual	Exposición que permanece después de aplicar controles.
Tratamiento	Acciones adicionales, responsables y plazos.
Indicadores de alerta	Datos o comportamientos que pueden revelar materialización.

Ejemplo de registro

CAMPO	CONTENIDO
Proceso	Gestión de proveedores y pagos
Escenario	Creación de proveedor ficticio y pago de facturas inexistentes
Actor	Empleado de compras en colusión con tercero
Método	Alta irregular, documentación falsa y cambio de cuenta
Impacto	Pérdida financiera, fiscal y reputacional

CAMPO	CONTENIDO
Controles	Segregación, verificación independiente y conciliación
Señales	Domicilios repetidos, cuentas compartidas, importes fraccionados
Riesgo inherente	**Alto**
Riesgo residual	**Moderado**
Tratamiento	Doble validación y analítica de coincidencias
Responsable	Dirección financiera
Revisión	Trimestral

Probabilidad e impacto

La valoración puede utilizar escalas cualitativas o cuantitativas.

El impacto debería considerar:

- Pérdida económica.
- Daño a clientes.
- Consecuencias legales.
- Interrupción operativa.
- Reputación.
- Seguridad.
- Impacto social.

No es suficiente aplicar una multiplicación mecánica. Un fraude poco probable puede ser crítico si amenaza la continuidad, la licencia o la confianza pública.

Riesgo inherente y riesgo residual

- **Riesgo inherente:** exposición antes de considerar controles.
- **Riesgo residual:** exposición después de considerar su eficacia.

Esta distinción permite determinar si el control realmente reduce el riesgo o solo existe documentalmente.

El mapa como herramienta viva

Debe actualizarse cuando:

- Se detecta un fraude.
- Cambian los procesos.
- Se introduce tecnología.
- Se contrata o externaliza una actividad.
- Se entra en un nuevo mercado.
- Se producen reorganizaciones.
- Aparecen nuevas tipologías.
- Un control falla.

— Cambian los incentivos.

El mapa orienta el presupuesto, las pruebas de controles, la formación, la analítica de datos y el plan de auditoría.

10 Síntesis normativa de ISO 37003:2025

La ISO 37003 propone que la organización establezca un Sistema de Gestión del Control del Fraude proporcional a su contexto, tamaño, actividades y exposición.

En esencia, recomienda:

PLANIFICAR · LIDERAR · SOPORTAR	PREVENIR · DETECTAR · RESPONDER · MEJORAR
01 Comprender el entorno y las expectativas de los interesados.	18 Probar la resistencia de los controles.
02 Delimitar el alcance del sistema.	19 Proteger tecnología, información y activos físicos.
03 Evaluar sistemáticamente los riesgos de fraude.	20 Implementar mecanismos de detección.
04 Involucrar al órgano de gobierno y a la alta dirección.	21 Utilizar analítica e inteligencia artificial con supervisión.
05 Aprobar una política de control del fraude.	22 Facilitar el reporte confidencial.
06 Asignar responsabilidades y autoridades.	23 Responder inmediatamente ante sospechas razonables.
07 Coordinar control del fraude, seguridad de la información y auditoría interna.	24 Preservar evidencia física y digital.
08 Establecer objetivos y planes.	25 Investigar con competencia, independencia e imparcialidad.
09 Proporcionar recursos y competencias.	26 Separar investigación y decisión disciplinaria.
10 Integrar el riesgo de fraude en los procesos de empleo.	27 Registrar, analizar y escalar los incidentes.
11 Formar al personal y, cuando corresponda, a terceros.	28 Gestionar crisis y comunicaciones.
12 Comunicar y promover el sistema.	29 Recuperar fondos o bienes cuando sea posible.
13 Controlar la información y preservar la confidencialidad.	30 Considerar el impacto sobre víctimas e interesados.
14 Diseñar controles preventivos.	31 Revisar los controles después de cada incidente.
15 Gestionar conflictos de intereses.	32 Medir y auditar el funcionamiento del FCMS.
16 Evaluar personal y socios de negocio según el riesgo.	33 Someterlo a revisión de la dirección.
17 Revisar incentivos y metas de desempeño.	34 Corregir deficiencias y mejorar continuamente.

La estructura completa y los contenidos operativos —prevención, detección, respuesta, auditoría y mejora— están reflejados en el articulado oficial de la norma.

11 Conclusiones

ISO 37003 supone un cambio de enfoque: el fraude deja de tratarse únicamente como un incidente que debe investigarse y pasa a gestionarse como un riesgo permanente de gobierno, cultura, procesos, personas y tecnología.

La norma no pretende que todas las organizaciones adopten los mismos controles. Propone un sistema proporcional, basado en riesgos y adaptado al contexto. Una empresa pequeña puede implementar medidas sencillas pero rigurosas; una organización multinacional necesitará sistemas, analítica y estructuras más complejas.

La eficacia del FCMS dependerá de cinco condiciones:

- Compromiso auténtico de la dirección.
- Evaluación realista de los riesgos.
- Controles que funcionen en la práctica.
- Capacidad de detectar y responder.
- Aprendizaje sostenido.

Implementar ISO 37003 no significa producir más documentación. Significa conseguir que el riesgo de fraude influya en la selección de personas y terceros, la asignación de accesos, el diseño de incentivos, la aprobación de operaciones, el tratamiento de alertas y las decisiones de gobierno.

La norma no elimina el fraude ni garantiza que no ocurrirá. Su verdadera aportación consiste en hacer que la organización sea más difícil de defraudar, más rápida para descubrirlo, más competente para responder y más capaz de evitar su repetición.

DIAGNÓSTICO INICIAL

¿Quieres evaluar el nivel de madurez de tu organización o implementar la ISO 37003?

Contáctanos para un diagnóstico inicial. theDUEco. instrumenta sistemas de gestión y los deja certificables: primero se sabe dónde está la exposición, después se construye el sistema, y solo entonces se lo somete a un auditor.

Lic. Luis María González Vicente, MBA
Representante Legal — theDUEco. S.R.L.
Cel. +591 77299739 · luismariagonzalez@thedueco.bo

Truth is assets. No hay compliance sin ética.

theDUEco. S.R.L.

Governance, Risk Intelligence & Compliance · Whitepaper técnico · v1.0 · Agosto 2026