



ASOCIACIÓN INTERNACIONAL PARA LA COOPERACIÓN EN
LA PREVENCIÓN DEL FRAUDE

~~LUNES~~
LAS MARTES CLASS DE ICPF
~~MIÉRCOLES~~
~~JUEVES~~
~~VIERNES~~

El Futuro de los Canales de Denuncia Digitales: Integración de IA y Estándares ISO (37001, 37002, 37008)

André Barrantes

Agenda

- **Panorama internacional del soborno y la corrupción.**
- **ISO 37001:** Dentro de un canal de denuncia
- **ISO 37008:** Dentro de un canal de denuncia
- **ISO 37002:** Sistema de gestión de denuncias
- **Canal de denuncia: Características generales**
- **Al aplicada a canales de denuncia:** Mejores practicas y ruta.



Costo promedio de fraude por industria

Fuente:

Reporte de las Naciones

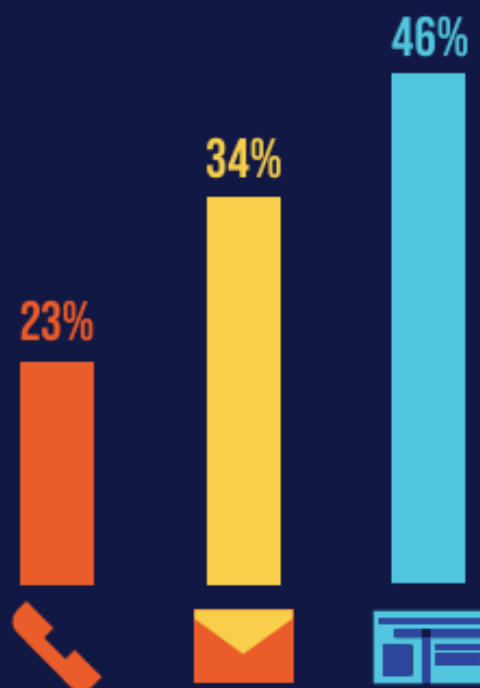
(2026 Report to the Nations), ACFE

The most **COMMON MECHANISMS** used to report fraud tips:



Email and web-based reports **BOTH** surpassed telephone hotlines.

- Telephone
- Email
- Web-based



Medios más utilizados para enviar denuncias

Fuente:

Reporte de las Naciones
(2026 Report to the Nations), ACFE

¿Cuál es el costo de **fraude** en las **organizaciones**?

El costo fraude total es alrededor del 5% de los ingresos brutos. Este costo puede implicar del 10 al 25% de la utilidad de un periodo.

El tiempo promedio de detección de fraude baja de 18 a 12 meses en organizaciones que cuentan con una línea ética.

Entre el 43% al 56 % de los fraudes se detectan por Canales de denuncia.



Beneficios Líneas éticas

- Reducción del tiempo de detección de fraude y por ende el costo del mismo.
- Evitar riesgos legales o reputacionales.
- Gestión de riesgos de fraude
- Mejora continua mediante planes de remediación
- Transparencia: Cumplimiento estándares internacionales

Estándares Internacionales de referencia

ISO 37001

Sistemas de Gestión Antisoborno.

ISO 37002

Sistemas de Gestión de Canales de Denuncia (Directrices)

ISO 37008

Directrices para las Investigaciones Internas en las Organizaciones

COSO

Marco Integrado de Control Interno

NOGAI

Normas Globales de Auditoría Interna

Un canal de denuncia dentro de la ISO 37001:

- **Accesibilidad y Facilidad de Uso:** Permite a empleados y partes interesadas reportar sospechas de soborno de manera rápida y sencilla desde cualquier lugar.
- **Confidencialidad y anonimato:** Garantiza que la identidad de los denunciantes se mantenga en secreto, lo que fomenta un ambiente de confianza y seguridad para realizar denuncias.
- **Eficiencia en la Gestión:** Facilita la recopilación y análisis de datos sobre incidentes, mejorando la capacidad de la organización para identificar riesgos y responder de manera oportuna.
- **Promoción de una Cultura Ética:** Alienta un entorno laboral transparente y responsable, donde se valoran la integridad y la ética en las prácticas empresariales.

Relación: ISO 37008 – Canal de denuncia

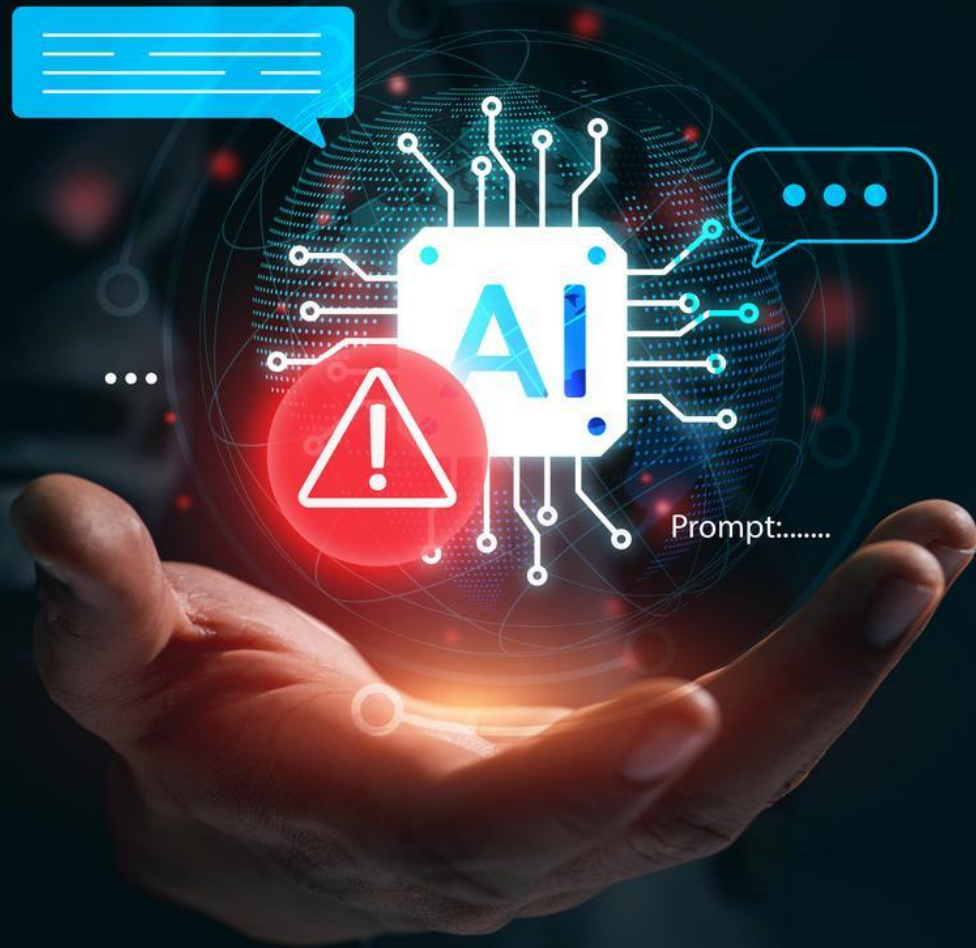
Un canal de denuncia es el medio por donde se reportan irregularidades dentro de una organización. La ISO/TS 37008 establece las directrices para investigar esas denuncias de manera ética, imparcial y efectiva. Juntos, aseguran que las denuncias se gestionen con confidencialidad y protección para los denunciantes. Esta combinación fortalece la transparencia y la confianza en la organización. Así, se promueve una cultura de cumplimiento y mejora continua.

ISO 37002: Sistemas de gestión de denuncias

Provee directrices para establecer, implementar, mantener y mejorar un sistema de gestión de denuncias efectivo y confiable dentro de una organización. Se relaciona con la norma ISO 37001 sobre sistemas de gestión antisoborno, pero atiende específicamente a los mecanismos de denuncia.

Objetivos principales de ISO 37002

- **Establecer una cultura de transparencia y confianza:** Crear un ambiente en el que los empleados y otras partes interesadas se sientan seguros y apoyados al reportar presuntos incumplimientos. **La socialización es clave en este objetivo**
- **Proporcionar una base normativa clara para establecer denuncias:** Instituir procedimientos claros y adecuados para la recepción, evaluación, y resolución de denuncias.
- **Proteger a los denunciantes:** Garantizar la confidencialidad, anonimato y protección contra represalias para quienes denuncian incumplimientos y/o irregularidades.
- **Garantizar una gestión efectiva de las denuncias:** Compromete una respuesta oportuna y adecuada a las denuncias, que incluya la investigación y toma de acciones correctivas según se requiera.



CONTEXTO ACTUAL:

CANALES DE DENUNCIA DIGITALES

- **Tecnología avanzada:** Canales de denuncia tecnológicos intuitivos y seguros.
- **Gobernanza y gestión de la ética:** Normativa interna integrada a ecosistemas digitales.
- **Sistemas de gestión:** Digitalizados y automatizados.
- **Socialización continua:** Sistemas de socialización integrados y automatizados.
- **Capacitación especializada:** Integrada a ecosistema digital línea ética.
- **Monitoreo y mejora continua:** Analítica de datos dinámica.
- **Aseguramiento:** Logs de auditoría automatizados.

Aplicación Inteligencia Artificial: Canales de denuncia digitales

INTELIGENCIA ARTIFICIAL

La misma **IA** que hoy alimenta la fábrica de **fraudes** es la única herramienta capaz de detenerlos. No estamos ante una crisis de seguridad, sino ante una **carrera por automatizar la confianza**. Quien no dote a su integridad de inteligencia, simplemente dejará de ver el fraude.



**Es hora de equiparar las fuerzas del bien
con las del mal en la lucha contra la corrupción**

CONTEXTO ACTUAL:

LA IA COMO INFRAESTRUCTURA

El error común es pensar que la **IA es una herramienta externa**.

El verdadero futuro de nuestra industria está en la **integración invisible**. No queremos que el oficial de cumplimiento aprenda a usar una IA; queremos que su software de siempre ahora tenga ojos, oídos y, sobre todo, criterio profesional.

LA CARRERA ARMAMENTISTA DE LA IA

En esta carrera, el atacante ya **automatizó** su maldad. Si el defensor sigue operando manualmente, el resultado es previsible. No estamos compitiendo contra personas, **estamos compitiendo contra algoritmos**. La única forma de ganar es convirtiendo nuestro canal en un **organismo inteligente**.



ARQUITECTURA DE CONFIANZA IA:

MITIGACIÓN RIESGOS



Soberanía de Datos (LLM Local):

Frente al riesgo de fuga de información en nubes públicas, se puede utilizar modelos Libres instalados en servidores propios. Sus denuncias nunca salen de su infraestructura; el cerebro de la IA vive donde viven tus datos.



Control de Acceso y Ejecución:

La IA no tiene libertad total. Se recomienda definir Tools específicas (conectores) que respetan las listas ACL (permisos). Por ejemplo, si un usuario no tiene permiso para ver un documento, la IA tampoco podrá consultarla para él.



Integridad de los datos:

Garantizar la veracidad mediante técnicas RAG junto con SKILLS, obligando a la IA a consultar la evidencia real antes de responder. Si el dato no existe en el expediente procesado, la IA no lo inventa; solo cita la realidad.

VISIÓN IA:

Corto Plazo (1 a 3 meses)

Interrogador de Normativa Interna:

Chatbot de precisión para la consulta inmediata de reglamentos, códigos de ética y protocolos. Elimina la búsqueda manual en documentos extensos, entregando respuestas con citas textuales de la norma.

Consultor de Capacitación Especializada:

Chatbot interactivo que transforma sesiones de **entrenamiento y material educativo** en una base de conocimientos 24/7. Permite resolver dudas complejas basándose en el contexto real de las capacitaciones impartidas.

VISIÓN IA:

Mediano Plazo (4 a 12 meses)

Agente Experto en Estándares Globales:

Integración a marcos internacionales. El chatbot no solo conoce tu empresa, sino que asesora sobre cómo los procesos actuales se alinean con las mejores prácticas globales de denuncia.

Inteligencia de Datos Unificada:

Acceso transversal a toda la base de conocimientos del sistema (archivos, histórico de capacitaciones y logs). La IA deja de analizar secciones aisladas para ofrecer una visión 360° de la cultura ética organizacional.

Transparencia y Trazabilidad Total:

Cada respuesta incluye referencias directas y metadatos útiles. El sistema indica exactamente la fuente, el documento o la sesión de capacitación de donde extrajo la información, eliminando la opacidad.

C

Conversation

2 files - Ready



Ask about your documents

Use the composer below to ask about 2 files in "Conversation".

cuales so|

I



VISIÓN IA:

Largo Plazo (12 a 18 meses)

Capacidad Ejecutiva Supervisada:

La IA evoluciona de responder consultas a ejecutar acciones directas en el sistema mediante lenguaje natural. El administrador delega tareas operativas a la IA, manteniendo siempre el control final.

Asistente Proactivo de Soporte:

El sistema no solo ejecuta; analiza la solicitud del usuario y sugiere la mejor práctica de cumplimiento antes de actuar. (Ej: Recomendar desactivar cuentas en lugar de borrarlas para preservar la integridad de los logs).

Confirmación de Acciones por Objetos (Buttons):

Implementación de una interfaz de decisión rápida. La IA presenta opciones claras de ejecución, minimizando errores humanos y garantizando que cada cambio sea consciente y auditado.

Retos:

Soberanía de los datos:

Exige operar sobre servidores seguros y aislados, evitando nubes públicas que pongan en riesgo la confidencialidad de la información corporativa.

Integridad de los datos:

Obliga a que el agente se confíe rígidamente al repositorio oficial autorizado, garantizando respuestas confiables y sin alucinaciones.

Controles de Acceso y ejecución:

Aplica esquemas granulares basados en la norma ISO/IEC 27001, asegurando que cada usuario consulte solo la información que le corresponde por su cargo.

Trazabilidad y logs de auditoría automáticos:

Demanda el registro automatizado de cada interacción del sistema, generando un historial transparente que respalde la rendición de cuentas.

Conclusiones:

- Buenas practicas de Gobernanza: Los estándares internacionales ISO 37001, 37002, 37008 se vuelven en bases científicas de referencias a la hora de implementar un canal de denuncia
- Las practicas tecnológicas deben estar alineados a los estándares internacionales
- El canal de denuncia digital debe estar configurado al sistema de gestión de la organización.
- Integrar AI en el canal de denuncia no es una opción, si no se implementa el riesgo de obsolescencia del canal de denuncia es alto.

“Actualmente los **canales de denuncias** nos ayudan a **detectar y prevenir el fraude**. Con la integración de la IA, podemos soñar con predecirlo. **Es hora de ganar esta guerra.**”

SG SHOGUN
MONITOR SYSTEM

Muchas gracias

Correo electrónico: andre.Barrantes@shogunmonitor.com



SHOGUN: Canales de denuncia digitales