

Conflictos de interés:

Cómo gestionarlos a tiempo en sistemas
de compliance y denuncias internas



Un conflicto de interés en el trabajo aparece cuando factores personales, financieros o relacionales pueden interferir —o parecer que interfieren— con la **objetividad de una decisión**.

No es necesario que exista una falta. De hecho, en la mayoría de los casos, el problema no es el conflicto en sí, sino su falta de gestión.

Para áreas de compliance, legales, recursos humanos y auditoría, esto plantea un desafío concreto: construir condiciones para que estos **riesgos se identifiquen, se declaren y se gestionen** antes de escalar. En ese punto, los sistemas de denuncias internos y las herramientas de gestión —desde políticas hasta plataformas digitales— empiezan a ocupar un lugar central.





Qué entendemos por **conflicto de interés** en el marco del compliance

Un conflicto de interés es el compromiso —actual o potencial— de la independencia de una decisión laboral.

Puede originarse en:

- Relaciones personales
- Intereses económicos
- Actividades externas
- Beneficios directos o indirectos

→ El punto clave no es la intención, sino el **impacto** —real o percibido— sobre la decisión.

Desde la lógica del cumplimiento normativo, especialmente en esquemas modernos de whistleblowing, esto implica algo más amplio: no solo prevenir conductas indebidas, sino también gestionar zonas grises que afectan la confianza organizacional.

Conflictos reales, potenciales y percibidos: por qué importa diferenciarlos

No todos los conflictos operan
de la misma manera:

Reales:

- Cuando ya están influyendo en una decisión

Potenciales:

- Cuando podrían influir en el futuro

Percibidos:

- Cuando terceros pueden interpretar un sesgo

Este último suele ser subestimado, **pero es central**. En contextos organizacionales complejos, la percepción puede tener tanto impacto como el hecho.

Por eso, las organizaciones que avanzan en esta agenda no se limitan a gestionar incumplimientos, sino que desarrollan mecanismos de reporte —incluyendo reportes anónimos— que permitan anticipar riesgos antes de que se materialicen.



Por qué los conflictos de interés son un **tema de sistema** y no de casos aislados

Incluso cuando las decisiones son técnicamente correctas:

- La legitimidad puede verse afectada
- Se debilita la confianza interna
- Se incrementa la exposición reputacional y legal

Esto es especialmente sensible en procesos como:

- Selección y promociones
- Contratación de proveedores
- Investigaciones internas
- Decisiones financieras

En estos contextos, los conflictos no gestionados operan como un riesgo estructural.

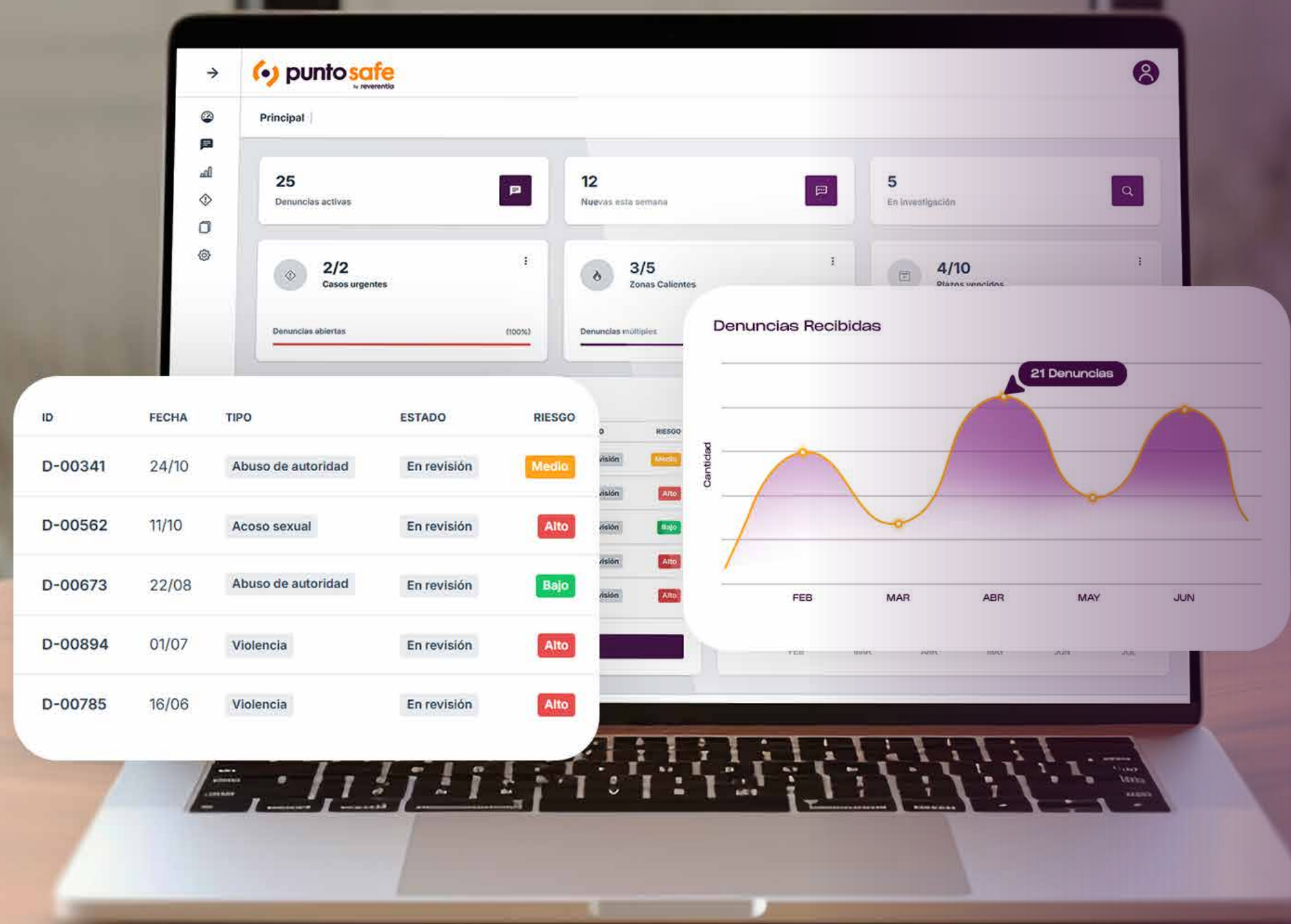
Por eso, las organizaciones más maduras en compliance empiezan a integrar su gestión dentro de plataformas de reportes o sistemas de denuncias, no como una vía punitiva, sino como un mecanismo de anticipación.

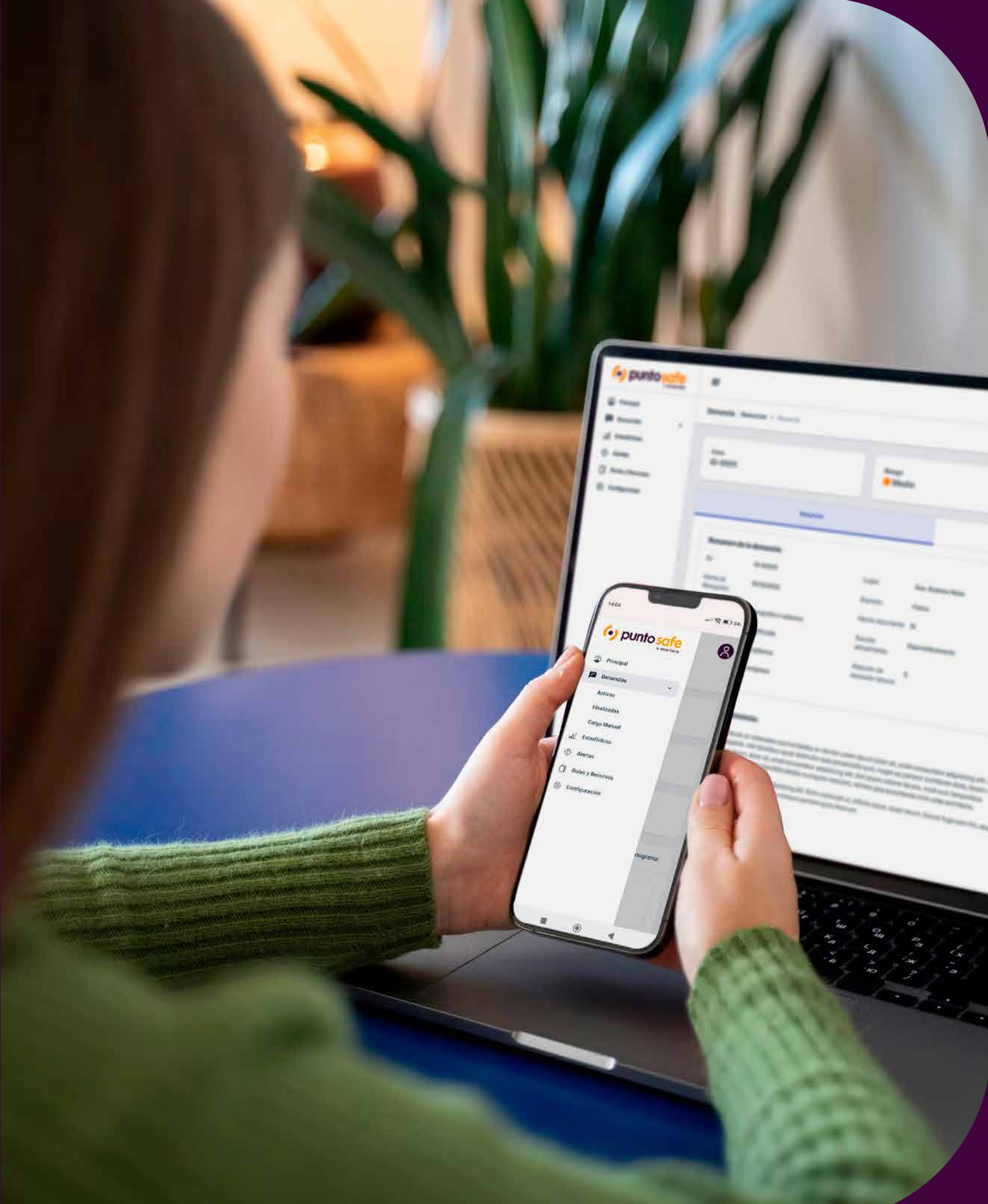
El rol de los canales de reporte en la gestión de conflictos

Tradicionalmente, los conflictos de interés se gestionaron a través de declaraciones juradas o reportes directos.

Hoy, la evidencia muestra que:

- Muchos conflictos no se declaran a tiempo
- Las personas dudan sobre qué constituye un conflicto
- Existe temor a consecuencias o a la exposición





En este escenario, los canales de denuncia internos y las plataformas de reportes empiezan a cumplir una **doble función**:

- 01 Permiten reportar situaciones potencialmente sensibles
- 02 Funcionan como espacios de consulta antes de que ocurra una decisión

Este segundo punto es clave: el sistema deja de ser reactivo y se vuelve preventivo.

- Para que esa función preventiva funcione, cada declaración debe aportar información suficiente para evaluar el riesgo. Un disclosure útil responde, como mínimo, cinco preguntas: quién declara, qué relación o interés se está informando, cuándo surgió, cómo podría incidir en una decisión y qué medidas se proponen para gestionarlo. Lo que conviene relevar incluye vínculos familiares o de pareja dentro de la organización, participación en empresas proveedoras, clientes o competidoras, cargos directivos o asesorías externas, trabajo paralelo, relaciones políticas o gremiales con impacto en el negocio, regalos, hospitalidades y viajes recibidos por encima de los umbrales internos, donaciones y patrocinios vinculados a intereses personales y procesos de búsqueda laboral con contrapartes.
- Tan importante como el contenido es la oportunidad. Un disclosure llega tarde cuando la decisión ya se tomó. Por eso conviene combinar tres modalidades: una declaración inicial al ingresar a la organización o a un nuevo rol, actualizaciones periódicas (anuales suele ser un piso razonable) y declaraciones ad hoc cada vez que aparece una situación nueva o cambia el contexto.
- En PuntoSafe, el canal de disclosure es un espacio donde el staff declara conflictos de interés actuales, potenciales o percibidos — antes de que se conviertan en un problema. Cada declaración queda registrada, trazada y disponible para el equipo de compliance con acceso controlado por usuario. Nadie externo accede.

Ejemplos de conflictos de interés: riesgos, señales y controles

Para equipos de compliance, legales, HR y auditoría, una de las mayores dificultades no es definir qué es un conflicto, sino identificarlo en la práctica y actuar con consistencia. Esta síntesis permite ordenar criterios y facilitar decisiones:

Situación	Riesgo principal	Señales de alerta	Controles habituales
Relación personal en línea de reporte	Favoritismo real o percibido	Ascensos o beneficios sin justificación clara	Cambio de reporte, intervención de HR, abstención en decisiones
Contratación de familiares (nepotismo)	Falta de equidad, debilitamiento de	Procesos poco transparentes, decisiones unilaterales	Procesos con panel, criterios documentados, restricciones
Trabajo paralelo con proveedor/cliente	Lealtades divididas	Preferencias reiteradas por un actor específico	Declaración previa, aprobación, restricciones
Participación financiera en proveedores	Beneficio económico personal	Presión por adjudicaciones o renovaciones	Umbrales de declaración, revisión independiente, abstención
Regalos u hospitalidad en contextos sensibles	Influencia indebida	Beneficios en momentos críticos (licitaciones)	Registro, límites, aprobación previa
Rol en organizaciones externas vinculadas	Uso indebido de información	Intercambio informal de datos estratégicos	Evaluación previa, restricciones, confidencialidad
Búsqueda laboral con contraparte	Decisiones sesgadas	Condiciones comerciales atípicas	Declaración, exclusión de negociaciones
Donaciones o patrocinios vinculados a intereses	Riesgo reputacional	Presión para aprobar ciertos destinos	Decisiones colegiadas, criterios objetivos

👉 **Clave operativa:**

No se trata de eliminar los conflictos, sino de hacerlos visibles, evaluarlos y aplicar controles proporcionales.

De la política al sistema: cómo gestionar conflictos de interés de forma efectiva

La gestión de conflictos no se resuelve con un formulario. Requiere un sistema.

Algunos elementos centrales:

- 01 Detección temprana**
Identificar relaciones, intereses financieros y roles externos relevantes.
- 02 Evaluación del riesgo**
No todos los conflictos tienen el mismo impacto. El contexto importa.
- 03 Definición de medidas**
Abstención en decisiones
Cambios en líneas de reporte
Supervisión adicional
- 04 Registro y trazabilidad**
La documentación es clave, especialmente frente a auditorías o investigaciones.
- 05 Monitoreo continuo**
Los conflictos evolucionan con los roles, los negocios y las relaciones. Por eso, además de actualizar las declaraciones, conviene revisar periódicamente las medidas de mitigación adoptadas y verificar si siguen vigentes.

- Sobre esa base, la gobernanza del proceso requiere definir, por escrito, tres niveles de responsabilidad. La recepción y registro suele estar a cargo de compliance o de la oficina de ética: garantiza confidencialidad, asienta la fecha de recepción y abre un expediente con número de caso. La evaluación combina el análisis del riesgo en función del cargo, la decisión que está en juego y la materialidad de la relación; aquí suele intervenir compliance junto con legales y, según el caso, con recursos humanos o auditoría interna. La decisión y seguimiento abarca la aplicación de medidas (abstención, recusación, supervisión adicional, cambio de línea de reporte, restricciones específicas) y su revisión periódica. Para casos sensibles, la decisión se eleva a un comité de ética o al órgano de administración.
- La trazabilidad sostiene esta arquitectura: registro fechado, criterios documentados, decisión fundada y archivo bajo plazos compatibles con la normativa aplicable. Cuando la persona involucrada tiene responsabilidad jerárquica o función pública, conviene además prever instancias de publicidad o reporte hacia órganos de control.
- En este proceso, contar con herramientas tecnológicas —como un software de gestión de denuncias o soluciones de whistleblowing— permite ordenar, sistematizar y dar consistencia a las decisiones.

Cultura organizacional, confianza y speakup

Uno de los principales obstáculos para gestionar conflictos de interés es que no se declaran.

Las razones suelen ser conocidas:

- Miedo a represalias
- Incertidumbre sobre si corresponde reportar
- Falta de claridad en los criterios

Cuando las personas perciben que:

- El sistema es confidencial
- Las decisiones son consistentes
- No hay consecuencias indebidas por

Por eso, las regulaciones más recientes —incluyendo marcos europeos vinculados a whistleblowing— hacen foco en un aspecto central: la no represalia.

Pero más allá de la norma, lo que define la efectividad del sistema es la confianza.

👉 Los conflictos aparecen antes.

El punto crítico: lo que no se declara, escala

En la práctica, la mayoría de los conflictos que terminan en problemas tienen algo en común:

- No fueron declarados a tiempo
- No había un canal claro para hacerlo
- O no había confianza en el sistema

En ese punto, el riesgo deja de ser potencial y **se vuelve real**.

La experiencia regional muestra un puñado de fallas que se repiten y conviene anticipar: tratar el disclosure como un trámite anual de firma masiva, sin lectura ni análisis; limitarlo a la alta dirección, dejando fuera mandos medios y áreas con poder de decisión sobre proveedores o personas; confundir confidencialidad con opacidad y no devolver a quien declara información sobre cómo se evaluó el caso; no actualizar las declaraciones cuando alguien cambia de rol, de jefatura o de unidad de negocio; carecer de criterios escritos para definir qué se considera material, lo que deja la decisión librada al juicio de quien recibe; almacenar las declaraciones en planillas dispersas, sin trazabilidad ni control de acceso; y omitir la articulación con los canales de denuncia, olvidando que quien reporta un conflicto ajeno también necesita protección.



De la gestión de conflictos a la gestión del riesgo organizacional

- Los conflictos de interés no fallan por falta de definición, sino por falta de sistema.
- Cuando dependen únicamente de declaraciones esporádicas o de la iniciativa individual, llegan tarde. Cuando no hay espacios claros para consultar o reportar, se silencian. Y cuando las decisiones no siguen criterios consistentes, la confianza se erosiona
- Por eso, cada vez más organizaciones están dando un paso adicional: pasar de políticas a sistemas. Integrar la gestión de conflictos dentro de sus procesos de compliance, apoyándose en canales de reporte confiables y herramientas que permitan ordenar, analizar y dar trazabilidad a la información.
- En ese contexto, soluciones como PuntoSafe no aparecen como un canal más, sino como una capa que hace operativo algo que muchas veces queda en lo declarativo:
 - la posibilidad de que las personas hablen a tiempo
 - consulten antes de decidir
 - gestionen situaciones sensibles con respaldo institucional.
- Porque, en definitiva, los conflictos de interés no son el problema.
- El problema es no tener un sistema que permita verlos antes de que se conviertan en un riesgo.

Disclosures de conflictos de interés en Latinoamérica: marco regulatorio y prácticas

El concepto de disclosure —la declaración formal de un interés que podría afectar la objetividad de una decisión— ocupa un lugar cada vez mayor en la regulación regional. Aunque cada país avanza a su ritmo, hay una línea común: el conflicto que no se declara termina convirtiéndose en una contingencia legal, reputacional y, muchas veces, sancionatoria.

A modo de referencia, conviene tener presentes algunos marcos:

Argentina: la Ley 27.401 de Responsabilidad Penal Empresaria establece que un programa de integridad debe contemplar reglas para identificar y manejar conflictos de interés. La Ley 25.188 de Ética en la Función Pública obliga a quienes desempeñan cargos públicos a presentar declaraciones juradas patrimoniales y de incompatibilidades.

Brasil: la Lei 12.846 (Lei Anticorrupção) y el Decreto 11.129/2022 exigen mecanismos internos de integridad, donde la gestión de conflictos y los canales de denuncia ocupan un rol central. La Lei 12.813 regula específicamente los conflictos de interés en el ámbito federal.

Chile: la Ley 20.393 sobre responsabilidad penal de las personas jurídicas y, más recientemente, la Ley 21.595 de Delitos Económicos, ampliaron la

exigencia de modelos de prevención. La Ley 21.643 (Ley Karin) reforzó además los canales internos de denuncia frente a hostigamiento y violencia laboral.

Colombia: la Ley 2195 de 2022 fortaleció el régimen de transparencia e integridad, e introdujo obligaciones específicas para entidades públicas y privadas en materia de programas de cumplimiento, canales de reporte y protección a quien denuncia.

México: la Ley General de Responsabilidades Administrativas regula el conflicto de interés en el sector público y exige declaraciones específicas. La Ley General del Sistema Nacional Anticorrupción articula además la obligación de las entidades de contar con políticas de integridad.

Perú: la Ley 30.424 incorporó la responsabilidad administrativa de las personas jurídicas y dio relevancia a los modelos de prevención. La Ley 31.227 trasladó al Contralor la administración de las declaraciones juradas de intereses.

Ecuador, Uruguay, Costa Rica, Panamá y República Dominicana: avanzan con reformas que recogen estándares de la Convención Interamericana contra la Corrupción y de la Convención de Naciones Unidas contra la Corrupción, donde la divulgación de intereses aparece como un pilar de prevención.

Más allá de la norma puntual, los estándares internacionales —ISO 37001, ISO 37301, lineamientos OCDE, principios de la Open Government Partnership— operan como referencia técnica al momento de diseñar un sistema de disclosures.

Disclosures y protección de datos: una tensión que conviene resolver desde el diseño

Las declaraciones de conflictos contienen datos personales y, en muchos casos, información sensible: vínculos familiares, situación patrimonial, afiliaciones, salud cuando incide en el rol. Las normas de protección de datos vigentes en la región —Ley 25.326 en Argentina, LGPD en Brasil, Ley 19.628 actualizada en Chile, Ley 1581 en Colombia, LFPDPPP en México, Ley 29.733 en Perú, Ley 18.331 en Uruguay— exigen tratar esa información con base legal, finalidad clara, minimización, plazos de conservación definidos y resguardos técnicos.

En la práctica, esto se traduce en cuatro prácticas mínimas: informar a quien declara para qué se usan sus datos y por cuánto tiempo se guardan; restringir el acceso al equipo que efectivamente interviene en el análisis; cifrar los repositorios y trazar cada consulta; y prever procedimientos para el ejercicio de derechos (acceso, rectificación, supresión cuando corresponda). Cuando la organización opera en varios países, conviene mapear las transferencias internacionales de datos y los acuerdos que las habilitan.

Terceros y partes relacionadas: el perímetro que más se subestima

Buena parte de los conflictos relevantes en la región se materializan a través de proveedores, distribuidores, agentes, consultoras y socios de negocio. Por eso, los disclosures internos pierden eficacia si no se complementan con un proceso de debida diligencia sobre terceros (third-party due diligence) que incluya identificación del beneficiario final, búsqueda en listas de sanciones y de personas expuestas políticamente, y declaración expresa de relaciones con quienes integran la organización.

En operaciones intracompañía y partes relacionadas, los marcos contables (NIIF/IFRS) y societarios exigen, además, la divulgación de transacciones en estados financieros. Articular el sistema de disclosures con el área de finanzas evita inconsistencias entre lo que la organización declara puertas adentro y lo que reporta hacia afuera.

Indicadores para medir si el sistema de disclosures está funcionando

Un sistema sin métricas no se gestiona, se intuye. Algunos indicadores que aportan información útil al comité de ética y al directorio:

Tasa de cumplimiento de la declaración inicial y de las actualizaciones anuales por área y por nivel jerárquico.
Tiempo promedio entre la recepción del disclosure y la decisión adoptada.

Proporción de declaraciones que derivan en alguna medida de mitigación, abierta por tipo de medida.

Cantidad de consultas previas al canal de ética (señal de uso preventivo, no solo reactivo).

Casos detectados por auditoría o por terceros que no habían sido declarados antes (indicador de subdeclaración).

Encuesta periódica de percepción sobre confianza en el canal y temor a represalias.

Estos indicadores conviene reportarlos con regularidad y ponerlos en contexto: una baja tasa de declaraciones puede leerse como buena gestión o como subreporte, según lo que muestren las demás métricas y los resultados de auditoría.

En conjunto, estas prácticas convierten a los disclosures en una herramienta viva, articulada con el resto del programa de compliance. Cuando el sistema funciona, la organización gana dos cosas que suelen escasear: información a tiempo para decidir y un lenguaje común para hablar de conflictos sin dramatizarlos ni minimizarlos.