

Guía para administradores de sistema de denuncia: El deber legal y la operación eficiente



Lo que debe saber, hacer y documentar quien administra un sistema de denuncias.

DIRECTIVA (UE) 2019/1937 · MÍNIMO LEGAL

- Define a quién y qué protege.
- Exige canales y plazos mínimos.
- Prohíbe represalias y exige remedios.
- Aplica mediante la ley nacional

ADMINISTRADOR DEL SISTEMA · 5 RESPONSABILIDADES

1. Controlar acceso y confidencialidad.
2. Cumplir acuse y feedback.
3. Asignar sin conflictos de interés.
4. Prevenir y vigilar represalias.
5. Conservar evidencia y mejorar el sistema.

ISO 37002:2021 · GESTIÓN EFICAZ IMPLEMENTACIÓN VOLUNTARIA

- 3 principios: confianza, imparcialidad y protección.
- 4 etapas para gestionar cada caso.
- Liderazgo, recursos, evaluación y mejora.
- Guía voluntaria; no es certificable.

REGLA DE ORO

Ley nacional aplicable + independencia y confidencialidad + evidencia proporcional.

EMPRESA PRIVADA

Regla general. Entidades menores pueden quedar incluidas por norma nacional o sectorial en sectores regulados como empresas financieras.

50+

trabajadores · umbral general

50–249 TRABAJADORES

Pueden compartir recepción e investigación si la ley nacional lo permite; cada entidad conserva confidencialidad, feedback y respuesta. No aplica si son más de 250 empleados.

SECTOR PÚBLICO

Entidades nacionales, regionales y locales; cada Estado puede prever excepciones limitadas para municipios o entidades pequeñas.

PERSONAS PROTEGIDAS

- | | |
|----------------------------------|-------------------------------------|
| ▪ Trabajadores y ex trabajadores | ▪ Voluntarios |
| ▪ Candidatos a un empleo | ▪ Contratistas y proveedores |
| ▪ Autónomos | ▪ Facilitadores |
| ▪ Accionistas y directivos | ▪ Personas o entidades relacionadas |



Canal de denuncias seguro, confidencial y trazable, alineado a la Directiva UE 2019/1937 e ISO 37002 — desplegable en 48 horas.

Requisitos del canal interno y plazos del procedimiento.

REQUISITOS DEL CANAL INTERNO

- Proteger la identidad del informante y de terceros mencionados.
- Impedir acceso de personal no autorizado.
- Admitir reporte escrito y oral; reunión física a solicitud.
- Designar persona o área imparcial para seguimiento.
- Dar seguimiento diligente y explicar canales externos.
- Tratar datos conforme al GDPR y registrar sólo lo necesario.
- Documentar llamadas/reuniones con consentimiento.

EVIDENCIA MÍNIMA DEL ADMINISTRADOR

- Sello de recepción
- Acuse y fecha
- Asignación / conflictos
- Acciones de seguimiento
- Fecha y contenido del feedback
- Historial de accesos

PROCEDIMIENTO INTERNO Y PLAZOS



PUNTO CLAVE

Feedback no significa necesariamente investigación concluida: informa la acción prevista o tomada y sus fundamentos.

TRES PRINCIPIOS RECTORES

01

CONFIANZA

El sistema es accesible, predecible, confidencial y genera credibilidad.

02

IMPARCIALIDAD

Las decisiones y la investigación se protegen de sesgos y conflictos.

03

PROTECCIÓN

Se previene y responde al perjuicio contra informantes y participantes.

Quiénes están cubiertos, qué represalias se prohíben y qué debe garantizar el administrador.

QUIÉNES PUEDEN ESTAR PROTEGIDOS

- Trabajadores y funcionarios públicos
 - Ex trabajadores y candidatos
 - Autónomos, accionistas y directivos
 - Voluntarios y practicantes
- Contratistas, subcontratistas y proveedores
 - Facilitadores, colegas y familiares relacionados
 - Entidades vinculadas al informante

REPRESALIAS PROHIBIDAS

- Despido, suspensión o degradación
 - Reducción salarial o cambio perjudicial
 - Disciplina, intimidación o acoso
 - Evaluación o referencia negativa
- Discriminación, lista negra o daño reputacional
 - Terminación contractual o pérdida de licencia
 - Amenazas, intentos y represalias indirectas

DEBERES DEL ADMINISTRADOR

- Identidad sólo bajo necesidad de conocer
 - Evaluar riesgo de represalia desde el ingreso
 - Separar y registrar quejas de represalia
 - Adoptar o escalar medidas de protección
- Excluir investigadores con conflicto
 - Proteger derechos y reputación de toda persona involucrada
 - Escalar de inmediato toda represalia alegada

CONDICIÓN BASE

Motivos razonables para creer que la información era verdadera y estaba dentro del ámbito; usar una vía protegida. Las reglas sobre anonimato varían por país.

HABILITADORES

Liderazgo y política · Roles y recursos · Competencia y comunicación · Controles operativos · Evaluación, auditoría y mejora

TRANSVERSAL A LAS 4 ETAPAS

La confidencialidad, la protección contra represalias y el registro proporcional atraviesan todo el proceso.



operado por AMITAI

Canal de denuncias seguro, confidencial y trazable, alineado a la Directiva UE 2019/1937 e ISO 37002 — desplegable en 48 horas.

El sistema debe demostrar qué hizo, quién lo hizo y cuándo

Checklist mínimo de gobierno, evidencia y supervisión para el administrador.

CONTROL	EVIDENCIA MÍNIMA	FRECUENCIA
Aplicabilidad	Registro legal por país, entidad y sector	Anual + cambios
Accesos	Matriz de roles y registros de acceso	Trimestral
Plazos	Recepción, acuse, acciones y feedback fechados	Cada caso
Conflictos	Declaración, revisión y reasignación	Cada caso
Datos	DPIA / privacidad, retención y borrado	Anual + caso
Represalias	Evaluación de riesgo y medidas protectoras	Continuo
Cierre	Resultado, acciones, responsables y verificación	Cada caso
Eficacia	KPI, auditoría, capacitación y mejoras	Trim. / anual

SEÑALES DE FALLA

- Buzón compartido sin control de acceso.
- Identidad revelada por conveniencia.
- Investigador dentro de la línea implicada.
- Acuse o feedback fuera de plazo.
- Retención indefinida de expedientes.
- Cierre sin protección ni remediación.

ESCALAR DE INMEDIATO

Riesgo de seguridad · destrucción de evidencia · alta dirección implicada · represalia.