

GUÍA OPERATIVA

# Checklist Corporate Compliance

8 pasos para implantar un programa eficaz  
bajo el art. 31 bis del Código Penal

Conforme a art. 31 bis CP, Ley 2/2023, UNE 19601 e ISO 37301



AUTOR

**Diego Molina**

Director · Molina Law Boutique

[molinalawboutique.es](http://molinalawboutique.es)

## CÓMO USAR ESTE CHECKLIST

## Implantar Corporate Compliance: idoneidad y eficacia

Desde la reforma del Código Penal (**LO 1/2015**), las personas jurídicas pueden ser penalmente responsables por delitos cometidos por administradores y empleados. Un **programa de compliance idóneo y eficaz** (art. 31 bis CP) puede eximir o atenuar significativamente esa responsabilidad.

Idoneidad significa que el programa cubre los riesgos reales del negocio. Eficacia significa que se ejecuta de verdad y deja **evidencias verificables**. Lo que jueces, fiscales y auditores externos comprueban no es el manual: es la **trazabilidad** de cada control.

Este checklist resume los **8 controles mínimos** que cualquier empresa debería tener cubiertos. Para cada uno encontrarás:

- **Qué debes hacer:** descripción operativa, no teórica.
- **Evidencia esperada:** el documento o registro concreto que necesitarás ante una inspección, una auditoría externa o un proceso de due diligence.

Si tienes dudas sobre cómo aterrizar alguno de los pasos en tu empresa, escríbenos: [diego@molinalawboutique.es](mailto:diego@molinalawboutique.es) o **+34 653 485 591**.

**+50**

empresas asesoradas

**24 h**

tiempo de respuesta

**31 bis CP**

+ UNE 19601 e ISO 37301

## PASOS 1 - 4

1

## Diagnóstico y mapa de riesgos

Identifica los riesgos legales, penales y regulatorios según actividad, sector, clientes, terceros y canal comercial. Documenta probabilidad, impacto y los controles existentes con un criterio defendible ante jueces, fiscales y auditores externos.

**Evidencia esperada:** Matriz de riesgos fechada con valoración inherente y residual, plan de acción con responsables, calendario de revisión y aprobación por dirección.

2

## Código ético y políticas internas

Define el estándar de conducta y las políticas específicas que lo aterrizan: anticorrupción, conflictos de interés, regalos y hospitalidad, competencia, terceros y controles de gastos. Las políticas deben ser cortas, claras y con flujos de aprobación reales que el equipo entienda y aplique.

**Evidencia esperada:** Código ético versionado, políticas firmadas por dirección, acuses de recibo de empleados y registros de revisiones periódicas.

3

## Canal de denuncias (Ley 2/2023)

Habilita un canal interno conforme a la Ley 2/2023 de protección del informante: confidencialidad, no represalias, plazos de tramitación, protocolo de admisión, investigación, medidas y cierre con trazabilidad. Obligatorio desde 50 trabajadores y para sectores específicos sin umbral.

**Evidencia esperada:** Política del canal, procedimiento de gestión, registro de comunicaciones recibidas, resoluciones motivadas y métricas anuales.

4

## Due diligence de terceros

Evalúa el riesgo de proveedores, intermediarios, agentes y partners antes de contratar. Incorpora cláusulas de compliance en contratos, valida pagos y servicios efectivamente prestados, y haz un seguimiento periódico de la relación.

**Evidencia esperada:** Ficha de evaluación del tercero, contratos con cláusulas de compliance, validaciones documentales y revisiones periódicas con fecha.

## PASOS 5 – 8

5

## Formación por perfiles

Formación práctica, por roles y orientada a situaciones reales (no formación genérica de 'una vez al año'). Combina formación inicial con refrescos periódicos, micro-casos, checklists para el día a día y registro detallado de asistencia.

**Evidencia esperada:** Plan anual de formación, materiales, registros de asistencia por rol, evaluaciones y evidencias de comprensión.

6

## Controles internos y supervisión

Implanta controles preventivos y detectivos: aprobaciones por importe, segregación de funciones, validación de pagos a terceros, monitoreo de incidentes y reporting con KPIs al órgano de administración para detectar brechas pronto.

**Evidencia esperada:** Matriz de controles con responsables, registros de aprobaciones, indicadores periódicos y actas del órgano de administración.

7

## Compliance Officer y gobierno

Designa formalmente al Compliance Officer con autonomía, recursos y línea de reporte clara al órgano de administración. Define el RACI del programa, la periodicidad de reuniones del comité y las consecuencias ante incumplimientos detectados.

**Evidencia esperada:** Nombramiento formal del Compliance Officer, RACI del programa, actas del comité y reporting documentado a dirección con KPIs.

8

## Auditoría y mejora continua

Audita el programa periódicamente (interno y/o externo), detecta brechas, ejecuta acciones correctivas y actualízalo ante cambios normativos o de negocio. La idoneidad y eficacia del programa (art. 31 bis CP) se demuestran con ejecución, no con manuales.

**Evidencia esperada:** Informes de auditoría con hallazgos, plan de remediación con plazos, KPIs y evidencias de acciones correctivas cerradas.

## SIGUIENTE PASO

## ¿Te ayudamos a implantarlo?

Si tras leer este checklist tienes dudas sobre cómo aterrizar alguno de los pasos en tu empresa, escríbenos. Diagnóstico inicial sin compromiso para mapear riesgos y proponer un plan por fases con hitos y evidencias.

EMAIL	<b><a href="mailto:diego@molinalawboutique.es">diego@molinalawboutique.es</a></b>
WHATSAPP	<b>+34 653 485 591</b>
WEB	<b><a href="https://molinalawboutique.es/corporate-compliance">molinalawboutique.es/corporate-compliance</a></b>
DIRECCIÓN	<b>C. de Pradillo, 5, Madrid</b>

*Este documento es de carácter informativo y no constituye asesoramiento jurídico específico. Cada caso requiere análisis individualizado.*