

CERTIFICA LEGAL

¿ESTÁ TU EMPRESA PROTEGIDA ANTE LA NUEVA LEY DE DELITOS ECONÓMICOS?

AUTODIAGNÓSTICO EXCLUSIVO

Para Directores, Gerentes y Fiscales en Chile

La Ley 21.595 eliminó el compliance “de papel”. Hoy, el “defecto de organización” se castiga con penas que van desde millonarios días-multa hasta la disolución de la sociedad.

Responde este test de 15 preguntas para evaluar el nivel de exposición penal real de tu empresa.

15 PREGUNTAS • 5 BLOQUES • 3 NIVELES DE RIESGO

Marca una alternativa por pregunta: A, B o C.

BLOQUE I · GOBERNANZA Y AUTONOMÍA DEL MODELO

1. ¿Cuál es el canal de reporte real del Oficial de Cumplimiento (Encargado de Prevención)?

- A) [Bajo Riesgo] Reporta directamente al Directorio o Comité de Auditoría, posee autonomía jerárquica y derecho a veto en operaciones sospechosas.
- B) [Riesgo Medio] Reporta a la Gerencia General o Gerencia de Finanzas, lo que genera eventuales conflictos de interés operacionales.
- C) [Riesgo Alto] No contamos con un Oficial de Cumplimiento designado, o el cargo lo ejerce un administrativo sin facultades reales de fiscalización.

2. ¿Cómo se asigna y ejecuta el presupuesto del Modelo de Prevención de Delitos (MPD)?

- A) [Bajo Riesgo] Cuenta con un presupuesto anual autónomo, auditable y aprobado directamente por el Directorio para capacitaciones y auditorías externas.
- B) [Riesgo Medio] El presupuesto depende de la aprobación de la Gerencia General caso a caso, limitando las revisiones imprevistas.
- C) [Riesgo Alto] No existe un presupuesto asignado al área de cumplimiento; los gastos se manejan como costos operativos generales.

3. ¿El Directorio de la empresa recibe y analiza informes periódicos de cumplimiento?

- A) [Bajo Riesgo] Sí, el Directorio sesiona trimestral o semestralmente de forma exclusiva para revisar el estado del MPD, dejando constancia detallada en actas legales.
- B) [Riesgo Medio] Se presenta un informe anual ejecutivo rápido, pero no se debaten ni minutan detalladamente las brechas detectadas.
- C) [Riesgo Alto] El Directorio solo firma la aprobación formal del modelo una vez al año (cumplimiento cosmético) o no recibe informes.

BLOQUE II · MATRIZ DE RIESGOS Y CATÁLOGO EXTENDIDO

4. ¿Cuándo fue la última actualización profunda de la Matriz de Riesgos Penales de la empresa?

- A) [Bajo Riesgo] Posterior a la entrada en vigencia plena de la Ley 21.595, incorporando el nuevo catálogo de más de 200 delitos socioeconómicos.
- B) [Riesgo Medio] Hace más de un año; contempla la Ley 20.393 clásica (cohecho, lavado, receptación), pero no las nuevas categorías.
- C) [Riesgo Alto] No tenemos una Matriz de Riesgos documentada, o se compró un formato genérico que nunca ha sido adaptado al giro real.

5. ¿Están mapeados los riesgos de la “Segunda Categoría” (delitos cometidos en el ejercicio de la actividad empresarial)?

- A) [Bajo Riesgo] Sí, controlamos rigurosamente delitos informáticos, infracciones medioambientales, delitos contra el mercado de valores y fraudes tributarios específicos de nuestra operación.
- B) [Riesgo Medio] Conocemos los riesgos, pero no se han traducido en controles operativos ni se han normado en el reglamento interno.
- C) [Riesgo Alto] Desconocemos qué figuras penales de la operación diaria de nuestros ejecutivos pueden activar la responsabilidad penal de la persona jurídica.

6. ¿Cómo evalúa la empresa su exposición a Delitos Medioambientales y Laborales bajo la Ley 21.595?

- A) [Bajo Riesgo] Existen auditorías técnicas periódicas sobre disposición de residuos, permisos sectoriales e higiene/seguridad laboral, integradas al compliance penal.
- B) [Riesgo Medio] Las áreas operativas y de prevención de riesgos manejan estos temas por separado, sin cruzar los hallazgos con el Oficial de Cumplimiento.
- C) [Riesgo Alto] No consideramos que las fallas de seguridad laboral o problemas de patentes ambientales sean un riesgo penal corporativo.

BLOQUE III · CONTROLES OPERATIVOS E INTERACCIÓN CON TERCEROS**7. ¿Cuál es el protocolo de control sobre el uso de “Caja Chica” o “Fondos por Rendir” en terreno o sucursales?**

- A) [Bajo Riesgo] Todo gasto debe estar bancarizado, respaldado por factura electrónica rastreable y cruzado con una lista de proveedores validados. Prohibido el uso de efectivo sobre 5 UF.
- B) [Riesgo Medio] Se aceptan rendiciones en efectivo con boletas genéricas o vales informales, siempre que no superen ciertos montos mensuales.
- C) [Riesgo Alto] Existe alta discrecionalidad en la entrega de dinero en efectivo para destrabar contingencias operativas urgentes en faena o municipalidades.

8. ¿Qué nivel de Debida Diligencia (Due Diligence) se aplica a proveedores, contratistas y socios comerciales?

- A) [Bajo Riesgo] Todo tercero crítico firma cláusulas penales de cumplimiento, pasa por revisión de listas de riesgo (búsqueda de antecedentes) y acepta auditorías ex-ante.
- B) [Riesgo Medio] Solo les exigimos firmar una declaración jurada estándar donde aseguran cumplir la ley, sin verificación independiente de sus antecedentes.
- C) [Riesgo Alto] Se contrata exclusivamente por criterios de precio y disponibilidad técnica, sin evaluar el historial normativo del proveedor.

9. ¿Cómo se regulan y registran las interacciones de los ejecutivos con funcionarios públicos o fiscalizadores del Estado?

- A) [Bajo Riesgo] Contamos con una Política de Relación con el Sector Público y Registro de Lobby estricta. Está prohibido cualquier regalo, invitación o donación.
- B) [Riesgo Medio] Se siguen las normas generales de la Ley de Lobby, pero no existe una prohibición corporativa interna respecto a cortesías, almuerzos o patrocinios menores.
- C) [Riesgo Alto] Los gerentes o gestores de proyectos manejan las relaciones institucionales con libertad y autonomía para agilizar trámites y permisos.

BLOQUE IV · CANALES DE DENUNCIA E INVESTIGACIONES INTERNAS**10. ¿El canal de denuncias de la empresa garantiza el anonimato real y el estándar anti-represalias?**

- A) [Bajo Riesgo] Operamos con una plataforma externa encriptada, independiente, que permite el anonimato bidireccional y cumple con las normativas de la Ley 21.595 y la Ley Karin.
- B) [Riesgo Medio] El canal es un correo electrónico institucional (denuncias@empresa.cl) administrado por la Gerencia de Personas o el Fiscal de la empresa.
- C) [Riesgo Alto] No tenemos un canal formal de denuncias; los problemas se comunican verbalmente a la jefatura directa de cada área.

11. ¿Cuenta la empresa con un procedimiento de Investigación Interna formalizado y alineado con los Derechos Fundamentales?

- A) [Bajo Riesgo] Sí, un protocolo escrito que define plazos, resguarda el artículo 5° del Código del Trabajo, aplica el test de proporcionalidad y asegura la cadena de custodia de la evidencia digital.
- B) [Riesgo Medio] Investigamos los incidentes de forma reactiva, basándonos en la experiencia del área legal o de RR.HH., pero sin actas de registro digital estandarizadas.
- C) [Riesgo Alto] Las investigaciones internas se resuelven de forma ejecutiva mediante la revisión directa de los computadores de los sospechosos y desvinculaciones inmediatas.

12. ¿Las capacitaciones del Modelo de Prevención de Delitos evalúan la efectividad del aprendizaje?

- A) [Bajo Riesgo] Se realizan talleres de casos prácticos por rol operativo con evaluaciones obligatorias aprobadas y registradas digitalmente.
- B) [Riesgo Medio] Se envía anualmente un PDF informativo o un video e-learning genérico que los trabajadores deben marcar como "leído/visto".
- C) [Riesgo Alto] No se han realizado capacitaciones sistemáticas sobre cumplimiento normativo penal en el último año a la totalidad del personal.

BLOQUE V · CIBERSEGURIDAD E INFRAESTRUCTURA DIGITAL

13. ¿Están regulados en el Reglamento Interno (RIOHS) los límites del monitoreo tecnológico del empleador sobre los activos de la empresa?

- A) [Bajo Riesgo] Sí, el RIOHS estipula claramente el carácter laboral de las cuentas de correo corporativas y los servidores, fijando el procedimiento lícito para auditorías.
- B) [Riesgo Medio] El reglamento prohíbe el uso personal de las herramientas, pero no detalla el protocolo legal que debe seguir la empresa para revisarlas sin vulnerar la privacidad.
- C) [Riesgo Alto] No hay mención al uso y fiscalización de activos informáticos en el Reglamento Interno de la compañía.

14. ¿La empresa cuenta con un Plan de Respuesta a Incidentes de Ciberseguridad que controle el impacto penal corporativo?

- A) [Bajo Riesgo] Sí, un protocolo que incluye el congelamiento forense de evidencia (copias bit-a-bit con Hash) y el flujo de reporte mandatorio ante el CSIRT/ANCI dentro de las primeras 3 horas.
- B) [Riesgo Medio] El área de informática maneja respaldos y contención de virus, pero el plan no contempla los plazos de notificación legal obligatoria ni la preservación pericial judicial.
- C) [Riesgo Alto] Ante un ataque informático, la instrucción operativa es formatear los equipos de inmediato para volver a operar lo antes posible, destruyendo los registros de logs.

15. ¿La Alta Dirección comprende el impacto patrimonial del sistema de “Días-Multa” de la Ley 21.595?

- A) [Bajo Riesgo] Sí, el Directorio y la Gerencia de Finanzas han valorizado el impacto económico que significaría una sanción basada en los ingresos diarios reales de la empresa.
- B) [Riesgo Medio] Saben que existen multas altas, pero calculan la contingencia bajo el esquema antiguo de topes fijos en Unidades Tributarias Mensuales (UTM).
- C) [Riesgo Alto] Se asume que las multas de compliance son costos menores que cubren los seguros de responsabilidad civil de directores y ejecutivos (D&O;).

RESULTADO Y LÓGICA DE CONVERSIÓN PARA LA WEB

Bloqueo de resultado: al responder la pregunta 15, la pantalla no muestra la puntuación directamente.

¡DIAGNÓSTICO PROCESADO EXITOSAMENTE!

Hemos detectado que tu organización presenta brechas críticas en [X] bloques normativos chilenos, lo que expone al Directorio a contingencias bajo la Ley 21.595.

Formulario de captura para desbloquear el PDF completo:

- Nombre Completo
- Correo Corporativo (validar que no acepte @gmail o @hotmail)
- Cargo (Director / Gerente General / Fiscal / Oficial de Cumplimiento)
- RUT de la Empresa (opcional, para prospección comercial avanzada)

ALGORITMO DE PUNTUACIÓN INTERNA

Riesgo Bajo	Mayoría de A	Estructura robusta. Recomendamos auditoría de mantenimiento.
Riesgo Medio	Mayoría de B o combinación A/B	Existen brechas operativas. Tu certificación formal ya no te protege ante la Fiscalía.
Riesgo Alto / Alerta Crítica	Mayoría de C o cualquier C en preguntas 1, 4, 7 o 14	Defecto de organización inminente. Urge intervención legal y rediseño de matriz.

Nota de implementación: Esta sección final contiene instrucciones para el desarrollo web y la lógica de captura/conversión. No corresponde al resultado individual de un usuario hasta que el cuestionario sea implementado y puntuado.