otec.cl / MATERIAL DE ESTUDIO

Sistema de Compliance

CURSO COMPLIANCE · UNIDAD 2

Guía de estudio independiente con teoría aplicada, criterios de control, mapa de riesgos, análisis jurídico y herramientas para la implementación.

Edición normativa: 13 de noviembre de 2026

Fuentes primarias: BCN / LeyChile e ISO. Material pedagógico; no sustituye asesoría jurídica para casos concretos.

Objetivo y ruta de aprendizaje

Comprender y aplicar los componentes de un sistema de compliance contextualizado a empresas chilenas: implementación, presupuesto, mapas de riesgos, gobierno corporativo, responsable independiente, reglamentos, denuncias y responsabilidad jurídica.

Ruta de estudio

01. Fundamentos y arquitectura del sistema

02. Implementación, recursos y costos

03. Mapas de riesgos y herramientas

04. Análisis de riesgos y gobierno

05. Responsable, independencia y reglamentos

06. Canal de denuncias y respuesta

07. Responsabilidad jurídica y cierre integrador

Criterio de lectura normativa

Identifique en cada tema la diferencia entre norma legal vigente, regulación sectorial, metodología oficial, referencia técnica y norma futura. En particular, el texto reformado de protección de datos cuya vigencia general comienza el 01-12-2026 no debe tratarse como vigente al cierre editorial.

01 Fundamentos y arquitectura del sistema

De la observancia a un sistema de gestión

Compliance es una función de gestión que procura identificar obligaciones aplicables, traducirlas en conductas y controles, comprobar su ejecución y corregir desviaciones. Su alcance abarca exigencias legales, regulatorias, contractuales y compromisos internos adoptados por la organización. No se reduce a un reglamento ni a un curso de inducción: exige decisiones, responsables, evidencia y revisión. Un sistema proporciona un ciclo verificable desde la identificación del riesgo hasta la mejora de los controles. En Chile, debe distinguirse el sistema amplio de cumplimiento del modelo de prevención de delitos (MPD) relevante para la Ley 20.393. Un MPD puede formar parte del sistema, pero no equivale a todas las obligaciones de cumplimiento.

Alcance, contexto y partes interesadas

El diseño comienza por entender giro, tamaño, complejidad, estructura de propiedad, filiales, terceros, geografías, contratos y procesos sensibles. Se identifican las fuentes de obligaciones y los actores afectados: trabajadores, clientes, proveedores, administración, directorio, reguladores y comunidad. Una matriz de obligaciones registra fuente, artículo o requisito, aplicabilidad, responsable, control, evidencia, periodicidad y última revisión. Una obligación legal se diferencia de una meta ética voluntaria; ambas pueden administrarse, pero no deben confundirse sus consecuencias. El sistema debe incorporar contratistas y agentes cuando sus actividades generen riesgos para la entidad.

GRC y las tres dimensiones de la gestión

Gobierno corporativo define quién orienta y supervisa; gestión de riesgos ordena incertidumbres que podrían afectar objetivos; compliance precisa obligaciones y comprueba su observancia. La integración GRC evita matrices duplicadas y reportes contradictorios. La primera línea ejecuta y controla operaciones; la segunda asesora, establece metodología y monitorea; la auditoría interna, cuando existe, ofrece evaluación independiente. Estos roles corresponden a un modelo de referencia organizacional, no a una imposición legal universal. La rendición de cuentas pertenece a la dirección, incluso si contrata asesoría externa.

Diseño proporcional

Una organización de veinte personas no requiere el mismo despliegue que un grupo empresarial multinacional. La proporcionalidad ajusta formalización, tecnología y personal al riesgo real; no autoriza omitir los componentes exigibles por ley. Una empresa pequeña puede utilizar matrices sencillas y asesoría externa, mientras una entidad compleja necesita segmentación por negocio, reportes periódicos y trazabilidad tecnológica. La evaluación del modelo considera, entre otros, giro, tamaño, complejidad, recursos y actividades, conforme al artículo 4 de la Ley 20.393.

02 Implementación, recursos y costos

Ruta de implementación en ocho fases

Primero se establece el mandato de la alta dirección. Segundo se delimita el universo regulatorio y contractual. Tercero se levantan procesos y terceros. Cuarto se evalúan riesgos inherentes y controles existentes. Quinto se prioriza un plan con dueños, fechas y recursos. Sexto se aprueban políticas, protocolos, canal y capacitación. Séptimo se instala monitoreo con indicadores y evidencias. Octavo se realizan evaluaciones independientes y ajustes. Cada fase produce documentos comprobables y decisiones aprobadas, en lugar de declaraciones genéricas de compromiso.

Diagnóstico de brechas y plan de remediación

El diagnóstico compara requisitos relevantes con prácticas observadas. Para cada brecha se establece evidencia, severidad, responsable, medida, plazo y condición de cierre. Una política publicada pero desconocida por el personal es una brecha de eficacia; un control aplicado sin registro es una brecha de trazabilidad. El plan distingue correcciones urgentes, controles transitorios y soluciones permanentes. La urgencia depende de exposición, gravedad e inexistencia de medidas compensatorias, no solo del costo de implementación.

Costos directos, indirectos y costo de no actuar

Los costos directos incluyen diagnóstico jurídico, personal responsable, capacitación, canal, herramientas, auditoría y asesorías especializadas. Los indirectos incluyen horas de operación, ajustes informáticos, cambios contractuales, documentación y revisiones. El costo de no actuar puede abarcar investigaciones, interrupción operacional, litigios, pérdida de contratos y sanciones cuando procedan. No existe un porcentaje único de presupuesto obligatorio para todo programa. Un análisis económico puede comparar costo de control con reducción de exposición, pero jamás convertir una estimación didáctica en garantía de ausencia de responsabilidad.

Presupuesto justificable: ejemplo didáctico

EJEMPLO DIDÁCTICO: Una empresa destina 36 jornadas internas al levantamiento de procesos, 24 a capacitación, 12 a revisión de controles y un servicio externo para evaluación periódica. Estas cantidades son supuestos de aprendizaje, no datos de mercado ni mínimos legales. El presupuesto debe detallar alcance y entregables; el directorio o administración debe aprobar recursos según atribuciones. Para evaluar la decisión se consideran riesgos residuales, plazos de ejecución, dependencia de proveedores y sostenibilidad del monitoreo.

LISTA OPERATIVA / Documento mínimo: mandato, matriz de obligaciones, mapa de procesos, plan de acción y cuadro de responsables.

03 Mapas de riesgos y herramientas

Qué es un mapa de riesgos

Un mapa de riesgos reúne escenarios concretos, causas, eventos, impactos, probabilidad, controles, propietarios y tratamiento. Debe poder responder: ¿qué podría ocurrir?, ¿en qué proceso?, ¿por qué?, ¿qué controles previenen o detectan?, ¿qué evidencia existe? Riesgo inherente representa la exposición antes de considerar controles; residual representa la exposición después de considerar su diseño y efectividad. La identificación no se limita al catálogo penal: incluye obligaciones laborales, privacidad, competencia, consumo y sectoriales aplicables.

Fuentes para identificar riesgos

Las entrevistas a responsables de compras, finanzas, ventas y recursos humanos revelan flujos reales. Los contratos, registros contables, incidentes, resultados de auditoría, denuncias, observaciones regulatorias y procedimientos de aprobación aportan evidencia. Un taller multidisciplinario confronta supuestos y descubre actividades ejecutadas fuera de los manuales. El mapa se actualiza ante nuevas operaciones, cambios de normativa, adquisiciones, externalización y hallazgos. No se debe copiar automáticamente la matriz de otra empresa.

Escalas y cálculo didáctico

Una escala de probabilidad de 1 a 5 y de impacto de 1 a 5 puede producir un índice orientativo mediante la multiplicación de ambos valores. Esta fórmula es una herramienta didáctica, no una fórmula exigida por la Ley 20.393 o ISO 31000. Es esencial definir anclas descriptivas: el valor 5 de impacto puede representar efectos jurídicos graves, interrupciones relevantes o daño significativo según criterios previamente aprobados. Dos riesgos con la misma puntuación pueden requerir tratamientos distintos cuando difieren en naturaleza de daño o obligaciones normativas.

Controles y pruebas de efectividad

Un control preventivo reduce la probabilidad del evento; uno detectivo permite advertirlo; uno correctivo establece respuesta y recuperación. Segregación de funciones, debida diligencia de terceros, aprobación dual, conciliaciones, monitoreo de pagos y trazabilidad contractual son ejemplos que deben adaptarse al proceso. No basta constatar que existe una política: se examina si el control está diseñado correctamente y si funcionó en muestras de operaciones. Se registran desviaciones, causa raíz, medidas y fechas de cierre.

Herramientas digitales y límites

Una hoja de cálculo con historial de versiones puede ser suficiente para una organización pequeña; sistemas GRC y tableros permiten flujos, alertas, permisos y reportes complejos. Ninguna herramienta reemplaza criterio profesional, actualización legal ni calidad de datos. Los accesos a información sobre denuncias requieren controles reforzados. Indicadores útiles incluyen controles vencidos, hallazgos repetidos, cobertura de formación, tiempos de remediación, expedientes pendientes y cambios normativos sin análisis de impacto.

LISTA OPERATIVA / Para cada riesgo: evento, proceso, causa, exposición inherente, controles, evidencia, riesgo residual, titular, fecha de revisión.

04 Análisis de riesgos y gobierno

Proceso completo de evaluación

Se define el contexto y criterio, identifica el escenario, analiza causas y exposición, estima probabilidad e impacto, evalúa controles, determina riesgo residual y selecciona tratamiento. Las respuestas usuales son evitar, reducir, compartir o aceptar dentro de límites aprobados; ninguna opción permite incumplir obligaciones legales. Se establecen responsable y fecha de revisión, y se comunica el resultado a quienes pueden decidir. ISO 31000:2018 es una referencia técnica para ordenar el proceso, no una certificación ni una ley chilena.

Caso de compras y conflicto de interés

EJEMPLO DIDÁCTICO: Una empresa contrata servicios de transporte y descubre que un ejecutivo participó en la evaluación de una oferta vinculada a un familiar sin declarar la relación. El riesgo no se resuelve únicamente con sancionar una persona: se revisan declaraciones, segregación de funciones, reglas de compras, validación de beneficiarios finales cuando resulte pertinente y monitoreo de excepciones. El análisis evita afirmar automáticamente la existencia de delito; requiere hechos, norma aplicable y evaluación de especialistas cuando corresponda.

Directorio: deber de supervisión y evidencia

En sociedades anónimas, la Ley 18.046 establece el marco de gobierno corporativo aplicable. El directorio debe abordar la exposición de la empresa con información suficiente y dejar trazabilidad de decisiones según régimen correspondiente. Una práctica robusta es aprobar apetito y tolerancias de riesgo, examinar reportes del sistema, exigir cierre de hallazgos críticos, asignar presupuesto y evaluar independencia de la función. Un tablero trimestral puede presentar riesgos prioritarios, evolución, incidentes, acciones vencidas y recursos; el período es una recomendación, no regla universal.

Escalamiento y decisiones informadas

Los límites de atribuciones deben describir qué decide cada línea y cuándo se eleva un asunto. Un incidente grave, posible conducta delictiva o interferencia de la dirección requiere procedimiento especial, preservación de evidencia y asesoría jurídica adecuada. El comité de riesgos no sustituye automáticamente al directorio; la forma jurídica y poderes vigentes determinan responsabilidades. La aceptación de riesgo residual se documenta con razones, plazo y medidas compensatorias; nunca se formula como autorización para infringir la ley.

05 Responsable, independencia y reglamentos

Función del oficial de cumplimiento

El título “oficial de cumplimiento” se utiliza con frecuencia, pero el artículo 4 de la Ley 20.393 se refiere a uno o más sujetos responsables de la aplicación de protocolos, dotados de adecuada independencia, facultades efectivas, acceso directo a la administración y recursos. En sectores regulados puede haber denominaciones y funciones específicas; deben examinarse por separado. Sus tareas comprenden coordinar la matriz, promover capacitación, examinar controles, reportar hallazgos, gestionar mejoras y resguardar trazabilidad. No concentra por sí solo toda la responsabilidad de cumplimiento.

Independencia real y gestión de conflictos

La independencia se mide por capacidad para informar hallazgos sin represalias, acceso a información y administración, recursos y facultades, no por un título en un organigrama. Si el responsable depende funcionalmente del área investigada, el modelo debe prever escalamiento alternativo. Se documenta su nombramiento, atribuciones, limitaciones y mecanismos de reemplazo. Un asesor externo puede apoyar el sistema, pero la entidad conserva su deber de implementación efectiva. La evaluación periódica independiente prevista en la Ley 20.393 exige evitar autoverificaciones presentadas como auditorías independientes.

Reglamento y política de compliance

El reglamento interno del programa especifica objeto, alcance, principios, mapa de responsabilidades, reglas de conflictos, gestión documental, debida diligencia, procedimientos de denuncia, investigación, sanciones y mejora. Debe coordinarse con contratos, reglamentos internos laborales y políticas sectoriales. En el marco del artículo 4 de la Ley 20.393, los protocolos, procedimientos y sanciones internas deben comunicarse a trabajadores y contemplarse en los instrumentos contractuales que exige la norma. La redacción debe separar incumplimientos internos, infracciones administrativas y posibles delitos.

Capacitación, comunicación y evidencia

Publicar una política no prueba conocimiento ni cumplimiento. El plan formativo se segmenta por exposición: compras trabaja alertas de proveedores; tesorería, pagos; ventas, relaciones con clientes y autoridades; dirección, supervisión y decisiones. Se registra cobertura, comprensión y refuerzos. Los contratistas sujetos a protocolos aplicables reciben información pertinente. Toda publicación debe contar con fecha, versión, responsable de revisión y canal de consulta, evitando divulgar datos sensibles de denuncias o investigaciones.

LISTA OPERATIVA / Punto de control: los nombramientos deben definir acceso directo, recursos, incompatibilidades y protocolo de escalamiento.

06 Canal de denuncias y respuesta

Diseño de un canal seguro

El canal permite comunicar preocupaciones con acceso claro, confidencialidad, no represalias y criterios de admisibilidad. La Ley 20.393 exige considerar canales seguros de denuncia dentro de los protocolos del modelo de prevención. La organización define recepción, registro, clasificación, tratamiento de conflictos de interés, medidas de protección, custodia documental, investigación y cierre. La promesa de anonimato debe corresponder a una capacidad técnica real; confidencialidad y anonimato son conceptos distintos.

Recepción, triaje y preservación

Una denuncia debe recibir identificador, fecha, clasificación y acceso limitado. El triaje diferencia urgencias de seguridad, asuntos laborales, riesgos regulatorios y posibles delitos. La evidencia se conserva respetando integridad, legitimidad de obtención y protección de datos. Una denuncia no acredita culpabilidad. El análisis inicial identifica medidas de resguardo y conflicto de intereses de investigadores. Para supuestos de acoso laboral o sexual debe aplicarse el procedimiento legal específico y no sustituirlo por el canal genérico de compliance.

Investigación justa y cierre

El procedimiento considera imparcialidad, registro de actuaciones, posibilidad de respuesta de involucrados según el marco aplicable, documentación de hechos, análisis de evidencia y revisión jurídica. Las decisiones se fundamentan en criterios consistentes; la respuesta puede incluir remediación de controles, medidas disciplinarias lícitas o derivación a autoridades cuando proceda. Se comunica al denunciante información compatible con confidencialidad y derechos de terceros. Indicadores como tiempos, reincidencia y causas raíz sirven para mejorar el sistema sin exponer personas.

Privacidad: régimen vigente y futuro

A fecha 13 de noviembre de 2026, la Ley 19.628 mantiene el régimen actualmente aplicable a tratamientos de datos personales, según versión vigente de BCN. La Ley 21.719, publicada el 13 de diciembre de 2024 y modificada por Ley 21.806 de 5 de febrero de 2026, establece una reforma general con entrada en vigor el 1 de diciembre de 2026. En consecuencia, sus obligaciones diferidas se describen aquí como NORMA FUTURA, no como exigencias ya vigentes. El programa debe preparar inventarios, accesos, retención y protocolos, y comprobar el régimen aplicable en la fecha de cada tratamiento.

LISTA OPERATIVA / Protocolo de recepción: registrar, proteger, clasificar, investigar con imparcialidad, decidir, comunicar y mejorar.

07 Responsabilidad jurídica y cierre integrador

Personalidad jurídica y tipos de responsabilidad

La persona jurídica posee esfera patrimonial y organización diferenciadas, pero ello no equivale a impunidad. Deben distinguirse responsabilidad civil por daños, responsabilidad administrativa por infracciones y responsabilidad penal en los supuestos expresamente previstos. Las personas naturales pueden responder además según su participación y régimen aplicable. Un mismo incidente puede abrir procedimientos distintos, con estándares probatorios y consecuencias diferentes. No toda infracción de compliance constituye delito ni toda pérdida empresarial genera responsabilidad penal.

Levantamiento del velo societario

La expresión inglesa usual es “piercing the corporate veil”, conocida como levantamiento del velo societario. Es una construcción doctrinal y jurisprudencial de uso excepcional para analizar situaciones en que la personalidad separada se instrumentaliza abusivamente, según las circunstancias y fundamentos jurídicos del caso. No es una consecuencia automática de tener filiales, deuda o una investigación. El análisis civil exige revisar hechos, fraude o abuso alegado, legislación y jurisprudencia pertinente. Debe evitarse afirmar una regla uniforme aplicable a todas las formas societarias.

Responsabilidad penal de personas jurídicas

La Ley 20.393 regula la responsabilidad penal de personas jurídicas dentro de su ámbito y catálogo legal. Tras la reforma de la Ley 21.595, su artículo 4 caracteriza la adecuación de un modelo de prevención efectivo mediante identificación de actividades riesgosas, protocolos y procedimientos con canales seguros y sanciones internas, responsables con independencia y medios, y evaluaciones periódicas por terceros independientes con mecanismos de mejora. El artículo 3 contiene las condiciones de atribución. La sola tenencia de un manual o certificación comercial no garantiza exención de responsabilidad; importan implementación y efectividad según caso.

Diferencias comerciales y evaluación de terceros

En relaciones comerciales, los riesgos pueden originarse en representantes, proveedores y entidades vinculadas. Es necesario examinar el vínculo, el proceso, la autonomía operativa y las circunstancias relevantes según el texto vigente del artículo 3 de la Ley 20.393. Debida diligencia significa preguntar por propietarios y beneficiarios cuando proceda, antecedentes pertinentes, condiciones contractuales, pagos, subcontratación, señales de alerta y seguimiento. El análisis no convierte todo incumplimiento contractual en delito; deriva oportunamente a especialistas cuando existen indicios relevantes.

Plan de revisión periódica

Un sistema maduro combina revisión de obligaciones, prueba de controles, análisis de denuncias, evaluación independiente y mejora documentada. Un informe ejecutivo debería indicar alcance, hallazgos, criticidad, planes, responsables, recursos y decisiones pendientes. El sistema no busca “riesgo cero”: procura prevenir, detectar y responder con evidencia verificable. El cierre de la unidad exige explicar decisiones difíciles, fundamentar prioridades y demostrar el efecto de los controles sobre escenarios reales.

Comparador de responsabilidades

El mismo incidente puede activar diversas respuestas, siempre con presupuestos normativos distintos.

Ámbito	Pregunta principal	Respuesta típica
Interno	¿Se incumplió una política o procedimiento?	Corregir, investigar y aplicar medidas válidas.
Civil	¿Hay daño o incumplimiento jurídicamente relevante?	Analizar reparación y responsables.
Administrativo	¿Se infringió una norma fiscalizada?	Tramitar según organismo competente.
Penal	¿Concurren los elementos legales de un delito y atribución?	Evaluación y procedimiento penal conforme a ley.

Microcaso de aplicación

EJEMPLO DIDÁCTICO. Una empresa detecta proveedores sin revisión previa, un conflicto de interés en compras y un reporte de pagos no conciliados. La acción razonable es preservar antecedentes, identificar procesos y responsables, clasificar exposición, revisar controles y elevar hechos relevantes por una vía independiente. El caso no permite concluir por sí solo que se haya cometido delito.

Indicadores para dirección

Proporción de controles efectivamente probados; hallazgos críticos con plan; días de atraso por remediación; acciones de capacitación por grupos expuestos; número de cambios normativos examinados. Estos indicadores se proponen como práctica de gestión, no como exigencia universal.

Ficha de auditoría normativa

Corte de verificación: 13-11-2026. Se indica fecha de última modificación registrada en BCN cuando aplica, sin confundirla con la entrada en vigor de las disposiciones modificadas.

Ley 20.393 — responsabilidad penal de personas jurídicas

Clasificación: Norma legal vigente. Publicación: 02-12-2009. Última modificación o revisión: 17-08-2023 · Ley 21.595. Artículos 1, 3 y 4; versión vigente desde 01-09-2024.

https://www.bcn.cl/leychile/Navegar?idNorma=1008668

Ley 21.595 — Ley de Delitos Económicos

Clasificación: Norma legal vigente. Publicación: 17-08-2023. Última modificación o revisión: 29-09-2025 · Ley 21.770. Versión vigente BCN desde 29-09-2025; revisar disposiciones de vigencia diferida previstas para 2027.

https://www.bcn.cl/leychile/Navegar?idNorma=1195119

Ley 18.046 — Ley sobre Sociedades Anónimas

Clasificación: Norma legal vigente. Publicación: 22-10-1981. Última modificación o revisión: 19-08-2025 · Ley 21.757. Gobierno de sociedades anónimas; versión vigente desde 01-01-2026.

https://www.bcn.cl/leychile/Navegar?idNorma=29473

Ley 19.628 — Sobre Protección de la Vida Privada

Clasificación: Norma legal vigente. Publicación: 28-08-1999. Última modificación o revisión: 10-11-2022 · Ley 21.504 (versión actualmente vigente). Distinguir del texto reformado de vigencia diferida a 01-12-2026.

https://www.bcn.cl/leychile/Navegar?idNorma=141599

Ley 21.719 — protección y tratamiento de datos

Clasificación: Norma futura (vigencia general diferida). Publicación: 13-12-2024. Última modificación o revisión: 05-02-2026 · Ley 21.806. Entrada en vigor general 01-12-2026 según BCN; no presentar obligaciones diferidas como vigentes.

https://www.bcn.cl/leychile/Navegar?idNorma=1209272

Ley 21.643 — prevención e investigación del acoso

Clasificación: Norma legal vigente (ámbito laboral). Publicación: 15-01-2024. Última modificación o revisión: 03-01-2025 · Ley 21.724. Regímenes especiales de denuncia y resguardo laboral; vigencia desde 01-08-2024.

https://www.bcn.cl/leychile/Navegar?idNorma=1200096

ISO 37301:2021 — Compliance management systems

Clasificación: Referencia técnica internacional. Publicación: 04-2021. Última modificación o revisión: Confirmada por ISO en 2026. Estándar técnico; no obligación legal general en Chile.

https://www.iso.org/standard/75080.html

ISO 31000:2018 — Risk management guidelines

Clasificación: Referencia técnica internacional. Publicación: 02-2018. Última modificación o revisión: Confirmada por ISO en 2023. Guía técnica de gestión de riesgos; no norma certificable.

https://www.iso.org/standard/65694.html

Glosario de consulta rápida

26 términos esenciales para revisar protocolos, informes y decisiones.

Apetito de riesgo · Nivel y naturaleza del riesgo que la organización decide asumir para lograr objetivos, sin habilitar incumplimientos legales.

Auditoría independiente · Revisión con independencia respecto del diseño y ejecución de controles evaluados.

Canal de denuncias · Mecanismo para recibir, registrar y tramitar alertas y reportes de conductas posiblemente irregulares.

Compliance · Sistema de dirección y controles orientado a cumplir obligaciones aplicables y compromisos asumidos.

Conflicto de interés · Situación en la cual un interés particular puede interferir o aparentar interferir con deberes organizacionales.

Control correctivo · Acción para remediar consecuencias, causas o fallas después de detectar un evento.

Control detectivo · Mecanismo que identifica señales o eventos posiblemente irregulares.

Control preventivo · Mecanismo destinado a disminuir la probabilidad de que ocurra un evento no deseado.

Debida diligencia · Verificación proporcionada de antecedentes y riesgos antes y durante relaciones o decisiones relevantes.

Directorio · Órgano de administración y supervisión de una sociedad anónima conforme a su régimen jurídico.

Efectividad operativa · Medida en que un control fue aplicado realmente y produjo el resultado previsto.

Escalamiento · Remisión documentada de hechos o decisiones a una instancia con atribuciones suficientes.

Evidencia · Registro íntegro y pertinente que permite comprobar la ejecución de un control o actuación.

GRC · Integración de gobierno corporativo, gestión de riesgos y compliance.

Independencia · Capacidad funcional de informar y actuar sin interferencias incompatibles con el rol.

Investigación interna · Proceso documentado y proporcionado para analizar hechos reportados respetando el marco aplicable.

Levantamiento del velo · Doctrina excepcional relacionada con el abuso de la separación patrimonial societaria.

Mapa de riesgos · Representación estructurada de escenarios, impactos, controles y respuestas.

Modelo de prevención de delitos · Conjunto de medidas relevantes para prevenir y detectar conductas delictivas en la entidad.

Obligación de cumplimiento · Exigencia legal, regulatoria, contractual o compromiso interno aplicable.

Oficial de cumplimiento · Denominación organizacional o sectorial para quien coordina funciones de cumplimiento.

Probabilidad · Estimación de posibilidad de ocurrencia de un evento bajo criterios definidos.

Riesgo inherente · Exposición analizada antes de valorar controles existentes.

Riesgo residual · Exposición que permanece después de considerar controles diseñados y operativos.

Tratamiento del riesgo · Selección e implementación documentada de medidas frente a un riesgo.

Trazabilidad · Posibilidad de reconstruir una actuación mediante registros y responsables.

Checklist de cierre

■ El alcance considera obligaciones legales, compromisos internos, procesos y terceros.

■ La matriz registra dueño de la obligación, control, evidencia y revisión.

■ Los riesgos críticos tienen escenarios y criterios de priorización verificables.

■ La administración asignó recursos y recibió reportes de hallazgos.

■ Los responsables del modelo tienen independencia, atribuciones y acceso suficientes.

■ Los protocolos y sanciones internos se comunican y se integran contractualmente cuando exige la norma.

■ El canal de denuncias tiene triaje seguro, gestión de conflictos y protección de información.

■ Las investigaciones consideran el régimen laboral y privacidad aplicables.

■ El plan contempla revisión por terceros independientes y mejora documentada.

■ La reforma de datos personales diferida al 01-12-2026 está identificada como norma futura al corte.

Conclusión

Un sistema de compliance útil no se mide por documentos acumulados sino por riesgos identificados, decisiones de gobierno, ejecución demostrable de controles y capacidad de corregir fallas. La lectura jurídica debe actualizarse ante nuevas normas, actividades o procedimientos.

Fin de la guía de estudio · otec.cl · Unidad 2