MONITOR DE COMPLIANCE EMPRESARIAL

En el marco de las nuevas exigencias que imponen obligaciones en materia de compliance a las empresas que operan en Chile, la Cámara de Comercio de Santiago (CCS) y Defontana han creado una herramienta de autodiagnóstico online con el objetivo de permitirles a éstas evaluar el nivel de cumplimiento normativo de sus organizaciones.

Con la reciente implementación de nuevas normativas, como la Ley de Delitos Económicos y la Ley Karin, entre otras, las empresas enfrentan mayores exigencias en materia de compliance. En este contexto, este instrumento se presenta como una solución accesible y efectiva para que las organizaciones puedan medir su nivel de cumplimiento, compararse con el promedio y adoptar las medidas necesarias para fortalecer su gestión en esta área.

Completada la primera generación de 438 empresas auto diagnosticadas durante el primer semestre de 2025, la CCS y Defontana han realizado la primera evaluación del proyecto a partir de los resultados obtenidos en esta etapa.

El presente informe sintetiza estos resultados, con el objetivo de proporcionar indicadores agregados respecto del estado de preparación de la empresa chilena ante estas nuevas exigencias.

Debido a que los datos recopilados representan a empresas que se han autodiagnosticado a través de este instrumento, los resultados presentados no representan necesariamente de forma estadística al universo empresarial, si bien contienen información diversa en términos de tamaño y sectores de actividad de las organizaciones.

CONTEXTO

Una serie de normativas recientes imponen un conjunto de obligaciones a las empresas en Chile, principalmente orientadas a la prevención de ilícitos, la protección de los trabajadores y la seguridad de la información.

La Ley Karin (Ley N° 21.643) modifica el Código del Trabajo para fortalecer la prevención, investigación y sanción del acoso sexual, laboral y la violencia en el trabajo. Entre las obligaciones que plantea esta normativa se encuentran la exigencia de elaborar e implementar un protocolo de prevención, modificar el reglamento interno de orden, higiene y seguridad para incorporar dicho protocolo, realizar actividades de formación para los trabajadores, evaluar los riesgos psicosociales que puedan afectar a sus colaboradores, establecer canales de denuncia, entre otras.

La Ley de Responsabilidad Penal de las Personas Jurídicas (Ley N° 20.393), en tanto, establece que las empresas pueden ser penalmente responsables por ciertos delitos cometidos por sus dueños, gerentes, ejecutivos principales, o cualquier persona que esté bajo su dirección y supervisión, siempre que el delito se cometa en beneficio de la empresa. Para eximirse de esta responsabilidad, las empresas deben implementar un Modelo de Prevención de Delitos, y designar un Encargado de Prevención de Delitos, entre otros.
Ley de Delitos Económicos (Ley N° 21.595), que modifica y amplía la Ley N° 20.393, establece un nuevo sistema de responsabilidad penal para personas jurídicas y amplía el catálogo de delitos por los cuales una empresa puede ser sancionada. Para ello impone la necesidad de actualizar el Modelo de Prevención de Delitos de las empresas, reforzar los controles internos, implementar canales seguros de denuncia, capacitar a sus colaboradores y realizar evaluaciones periódicas por terceros independientes como atenuantes de responsabilidad penal.

La Ley Marco de Ciberseguridad (Ley N° 21.663), por su parte, establece una institucionalidad en materia de ciberseguridad y protección de la infraestructura crítica de información. Esta normativa impone a las empresas la obligación de realizar una evaluación de riesgos, identificando sus sistemas críticos, vulnerabilidades y brechas de seguridad, elaborar políticas de seguridad, implementar un plan de respuesta a incidentes, reportarlos, designar un encargado de ciberseguridad y realizar auditorías periódicas, entre otras.

PRINCIPALES RESULTADOS:

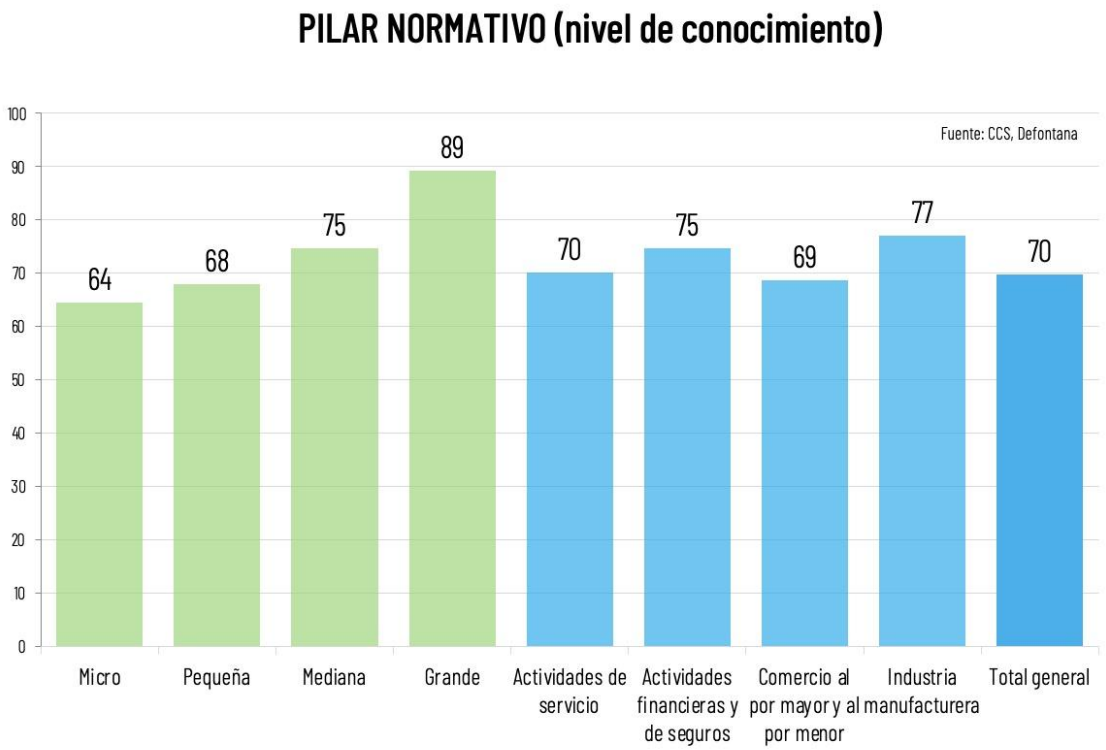
Resumen del indicador

El índice de compliance empresarial se estructura mediante tres dimensiones complementarias que capturan diferentes aspectos de la madurez organizacional en materia de cumplimiento: el pilar normativo, de equipo de trabajo, y de procedimientos y protocolos.

Los resultados preliminares revelan asimetrías estructurales y brechas de implementación entre distintos segmentos empresariales, evidenciando un patrón de desarrollo desigual que refleja tanto las limitaciones de recursos de las empresas más pequeñas como las diferencias sectoriales en la adopción de marcos de cumplimiento normativo.

El pilar normativo mide el nivel de conocimiento declarado por las empresas respecto al marco regulatorio aplicable, representando la dimensión cognitiva del compliance empresarial.

Los resultados evidencian una correlación positiva entre el tamaño empresarial y el conocimiento normativo, con un promedio general de 70 puntos sobre un máximo de 100. Las microempresas presentan un índice de 64 puntos, que luego se eleva a 68 y 75 puntos en el caso de las pequeñas y medianas empresas, para alcanzar sus máximos en el caso de las grandes (89 puntos). La brecha de 25 puntos entre microempresas y grandes empresas sugiere la existencia de economías de escala en la adquisición y procesamiento de información regulatoria.

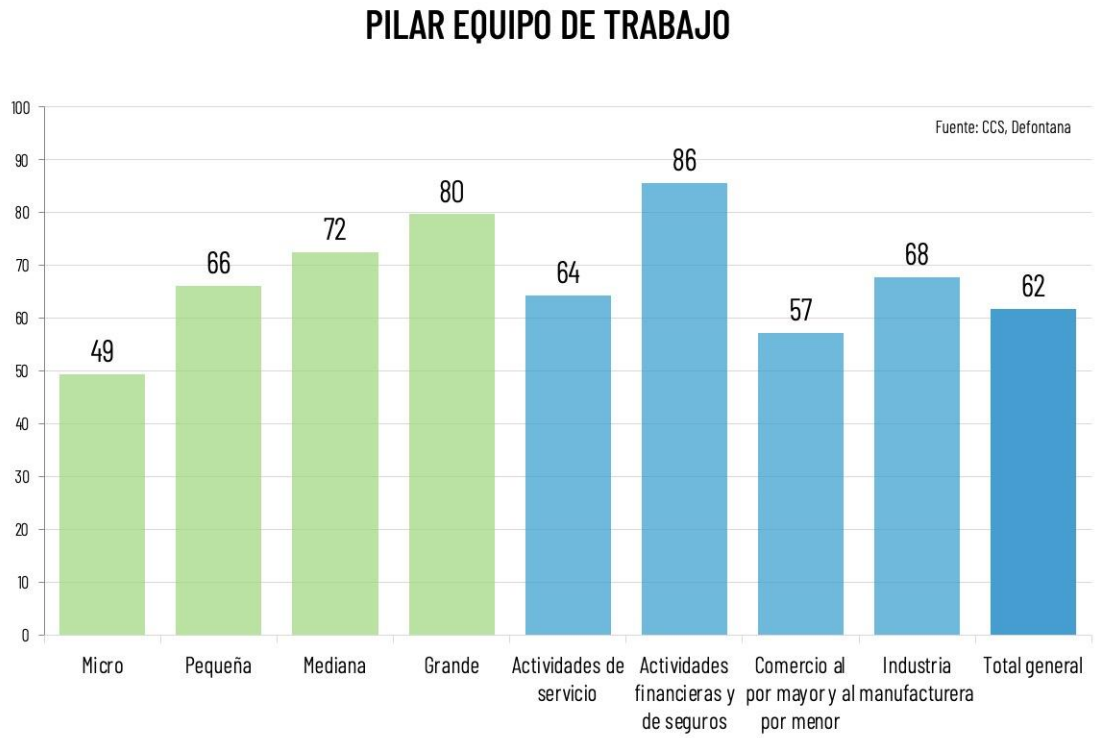


A nivel de sectores también se observan algunas heterogeneidades, con la industria manufacturera alcanzando 77 puntos, seguida por actividades financieras y de seguros (75), actividades de servicio (70) y comercio al por mayor y menor (69). Esta distribución refleja tanto la intensidad regulatoria sectorial como los requerimientos específicos de compliance en industrias altamente reguladas. La proporción de empresas de menor tamaño en cada sector también condiciona los resultados.

El nivel relativamente alto del pilar normativo (70% promedio), indica que la difusión de información regulatoria ha sido relativamente efectiva en términos agregados. Sin embargo, la brecha inter-empresarial sugiere que las asimetrías informativas y de

capacidades financieras constituyen una barrera significativa para el compliance uniforme en el tejido empresarial chileno.

El pilar de equipo de trabajo, por su parte, evalúa la presencia de recursos humanos dedicados o especializados en funciones de compliance, representando la dimensión organizacional del cumplimiento normativo.



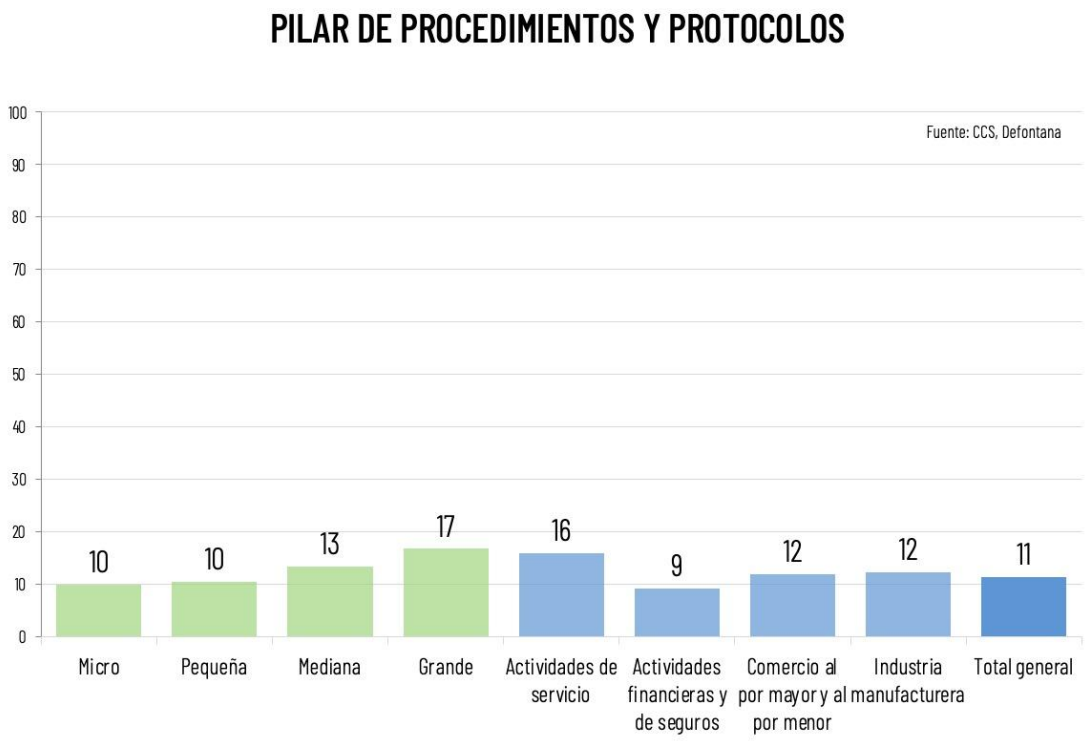
Esta dimensión presenta un promedio de 62 puntos sobre 100, también con una distribución fuertemente estratificada por tamaño empresarial. Las microempresas alcanzan la menor puntuación, con 49 puntos, mientras que las grandes empresas lideran con 80 puntos, generando una brecha de 31 puntos, la más amplia entre los tres pilares analizados.

A nivel sectorial, las actividades financieras y de seguros alcanzan el máximo puntaje en esta dimensión, con 86 unidades, lo que resulta consistente con los requerimientos regulatorios específicos del sector. En contraste, el comercio al por mayor y menor presenta el menor desarrollo (57 puntos), por detrás de actividades de servicio (64) e industria manufacturera (68).

La amplia brecha observada en este pilar refleja las limitaciones de recursos humanos especializados en empresas de menor escala. La estructura de costos fijos asociada a la contratación de personal especializado en compliance genera barreras de entrada

significativas para las PYMES, creando vulnerabilidades sistémicas en el cumplimiento normativo.

El pilar de Procedimientos y Protocolos, en tanto, mide la existencia de procedimientos formales, protocolos documentados y marcos institucionales estructurados para la gestión del compliance empresarial.



Esta dimensión presenta el desarrollo más limitado, con un promedio general de apenas 11 puntos sobre 100. Esta cifra revela una profunda brecha entre con el conocimiento normativo reportado (70 puntos), evidenciando la necesidad de avanzar de manera efectiva en la incorporación del marco regulatorio.

En este caso las grandes empresas alcanzan solo 17 puntos, mientras que las micro y pequeñas empresas registran 8 puntos, generando la menor brecha absoluta (9 puntos porcentuales), pero también los niveles más bajos de desarrollo institucional.

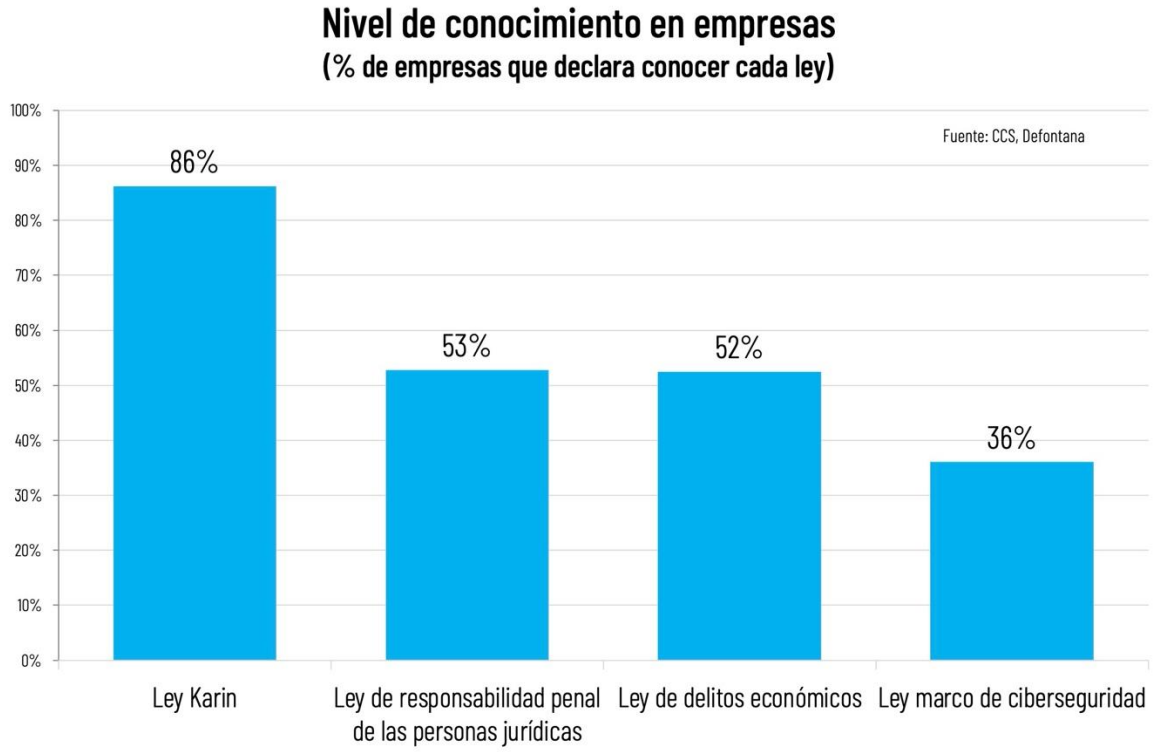
Por sectores, las actividades de servicio lideran con 16 puntos, seguidas por comercio e industria manufacturera (ambos 12), mientras que el sector financiero, presenta el menor desarrollo en esta área (9 puntos) a pesar de su liderazgo en otros pilares.

Los bajos niveles generalizados en este pilar indican que el compliance empresarial chileno permanece en una etapa incipiente de institucionalización, lo que

probablemente se relaciona con lo reciente de algunas normativas relevantes, por lo que las organizaciones se encuentran en etapa de adaptación a ellas. Esto sugiere que en los próximos trimestres este indicador debiera subir de manera relevante.

Nivel de conocimiento de leyes por parte de las empresas

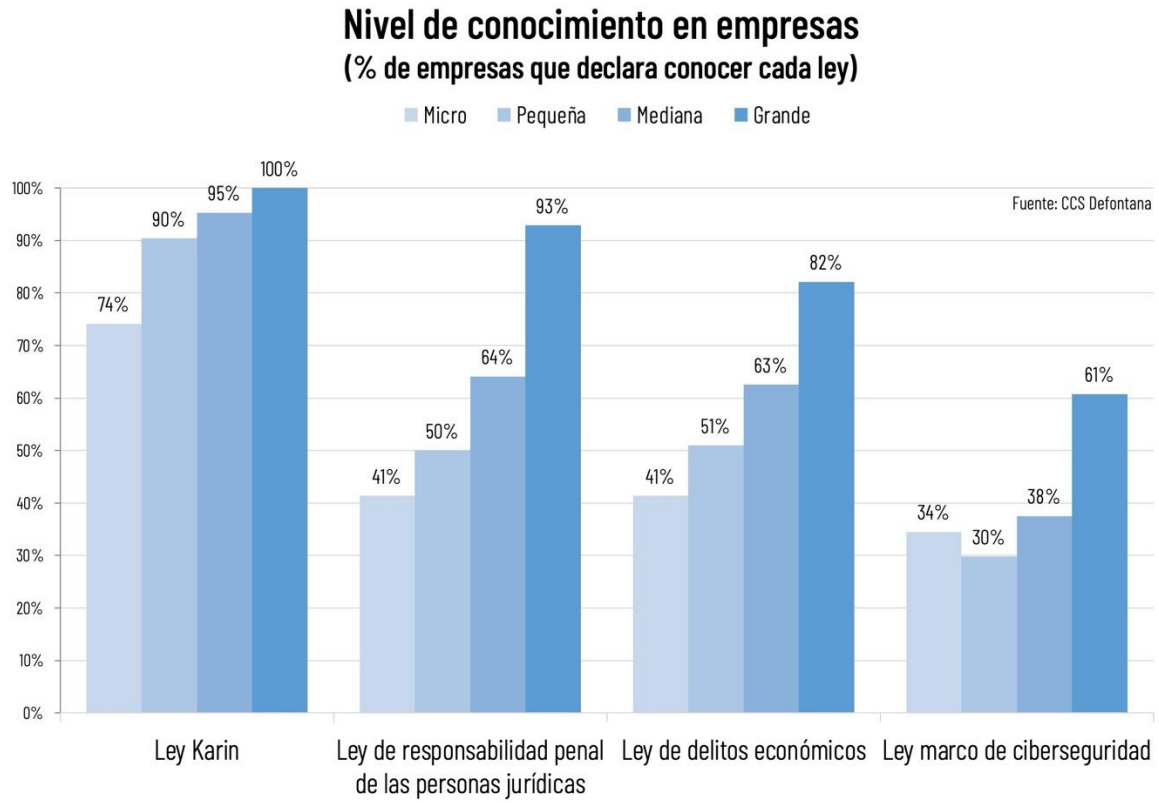
Los datos revelan una marcada heterogeneidad en el conocimiento normativo empresarial. La Ley Karin presenta el mayor nivel de reconocimiento con un 86% de las empresas encuestadas, seguida por la Ley de Responsabilidad Penal de las Personas Jurídicas (53%) y la Ley de Delitos Económicos (52%), ambas con un nivel de conocimiento intermedio. La Ley Marco de Ciberseguridad presenta la menor penetración, con apenas 36% de conocimiento entre las firmas de la muestra.



Esta distribución sugiere un patrón de adopción normativa que refleja tanto la antigüedad de las regulaciones como su impacto mediático y coercitivo. La alta prevalencia de conocimiento sobre la Ley Karin puede atribuirse a su reciente promulgación y amplia cobertura mediática, mientras que el bajo conocimiento sobre ciberseguridad indica una brecha significativa en la preparación empresarial ante riesgos digitales emergentes.

Los datos evidencian, además, una correlación positiva robusta entre el tamaño empresarial y el conocimiento normativo. Las grandes empresas alcanzan niveles de

conocimiento cercanos o iguales al 100% en Ley Karin y Responsabilidad Penal (100% y 93% respectivamente), mientras que las microempresas presentan los menores niveles en todas las categorías normativas. Particularmente notable es la brecha en ciberseguridad, donde las grandes empresas triplican el conocimiento de las micro y pequeñas empresas (61% vs. 34% y 30%, respectivamente).



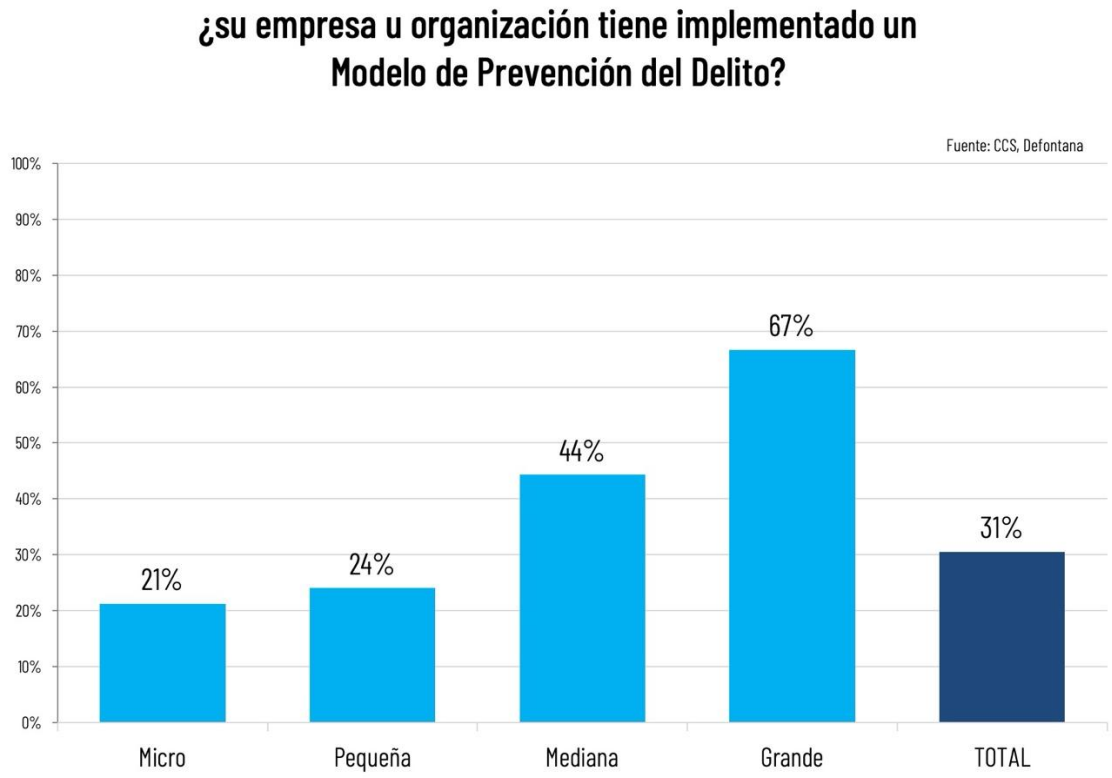
Esta segmentación refleja las economías de escala en la gestión del conocimiento legal y los recursos diferenciados para compliance. Las empresas grandes poseen mayor capacidad de inversión en asesoría especializada y sistemas de información legal, así como mayores sanciones por incumplimiento, mientras que las microempresas enfrentan restricciones de recursos que limitan su capacidad de actualización normativa. Esta asimetría genera potenciales riesgos de cumplimiento diferenciados según el tamaño empresarial.

Implementación de Modelos de Prevención del Delito

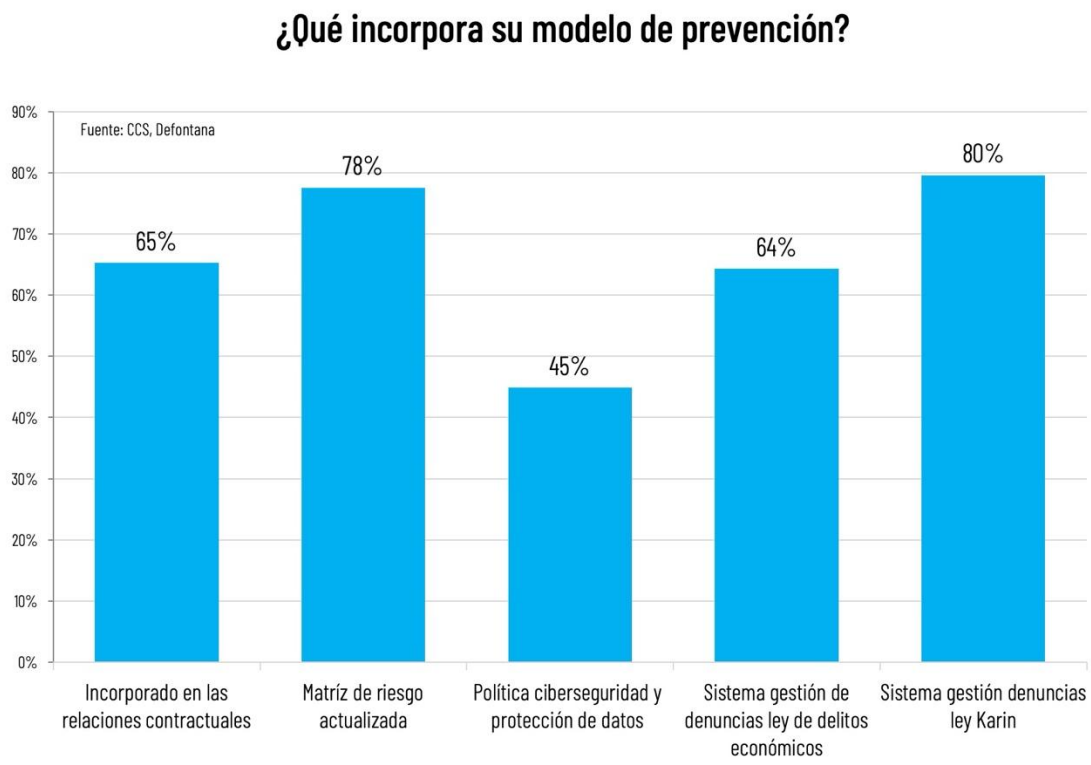
Los resultados revelan una implementación del modelo de prevención del delito altamente estratificada por tamaño. Las empresas grandes presentan una tasa de implementación del 67%, contrastando significativamente con las microempresas (21%). El promedio general de implementación del 31% indica que aproximadamente

dos tercios de las empresas chilenas no han materializado sistemas formales de prevención en esta área.

La baja tasa agregada de implementación sugiere la existencia de barreras económicas para la adopción de modelos de prevención del delito. Los costos fijos de implementación y mantenimiento de estos sistemas generan una mayor adopción en empresas de mayor escala, creando una brecha de compliance que puede traducirse en riesgos asimétricos de exposición legal y reputacional en el mercado.



El análisis de los contenidos de los modelos de prevención revela una priorización hacia sistemas de gestión de denuncias, con la Ley Karin liderando (80%), seguida por la matriz de riesgo actualizada (78%). Los componentes contractuales (65%) y los sistemas de gestión de denuncias de delitos económicos (64%), presentan niveles intermedios, mientras que las políticas de ciberseguridad y protección de datos muestran la menor incorporación (45%).

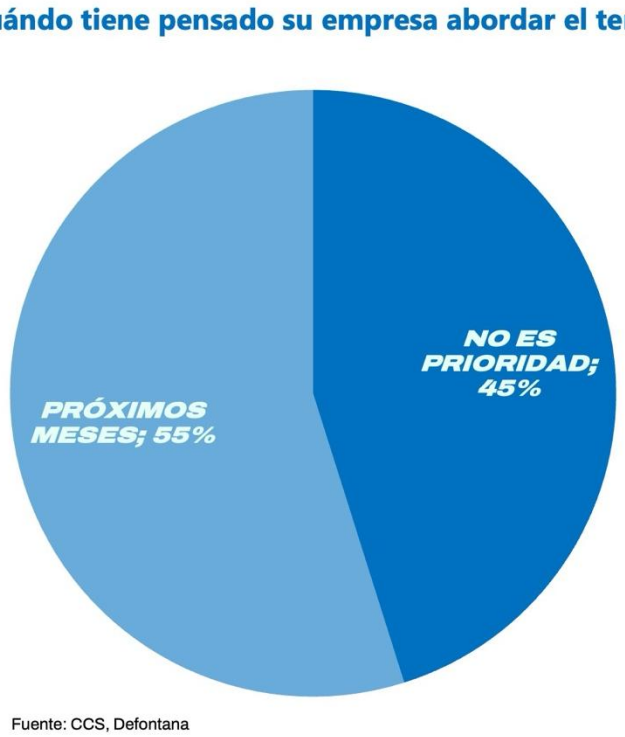


Esta distribución refleja un posible enfoque reactivo hacia el compliance, privilegiando mecanismos de detección y respuesta sobre estrategias preventivas. La baja integración de ciberseguridad sugiere una subestimación de riesgos digitales o limitaciones en la capacidad técnica para abordar estas amenazas emergentes.

En general, estos resultados sugieren que los esfuerzos de compliance se han centrado en cumplir con requisitos legales explícitos –como establecer canales de denuncia obligatorios– más que en adoptar herramientas integrales de gestión de riesgos. La alta prevalencia de sistemas de denuncia obedece claramente a las exigencias normativas recientes, mientras que elementos más estratégicos (matrices de riesgo, políticas contractuales), parecen estar menos difundidos. Fortalecer estos componentes rezagados sería importante para consolidar una cultura de integridad corporativa más robusta y mitigar riesgos de manera integral.

Prioridad otorgada al cumplimiento normativo por las empresas

El sentido de urgencia ante la necesidad de implementar modelos de prevención del delito no está claramente difundido. Un 45% de las empresas que no lo ha hecho declara que no se trata de una prioridad, mientras que el restante 55% planea implementarlos en los próximos meses.

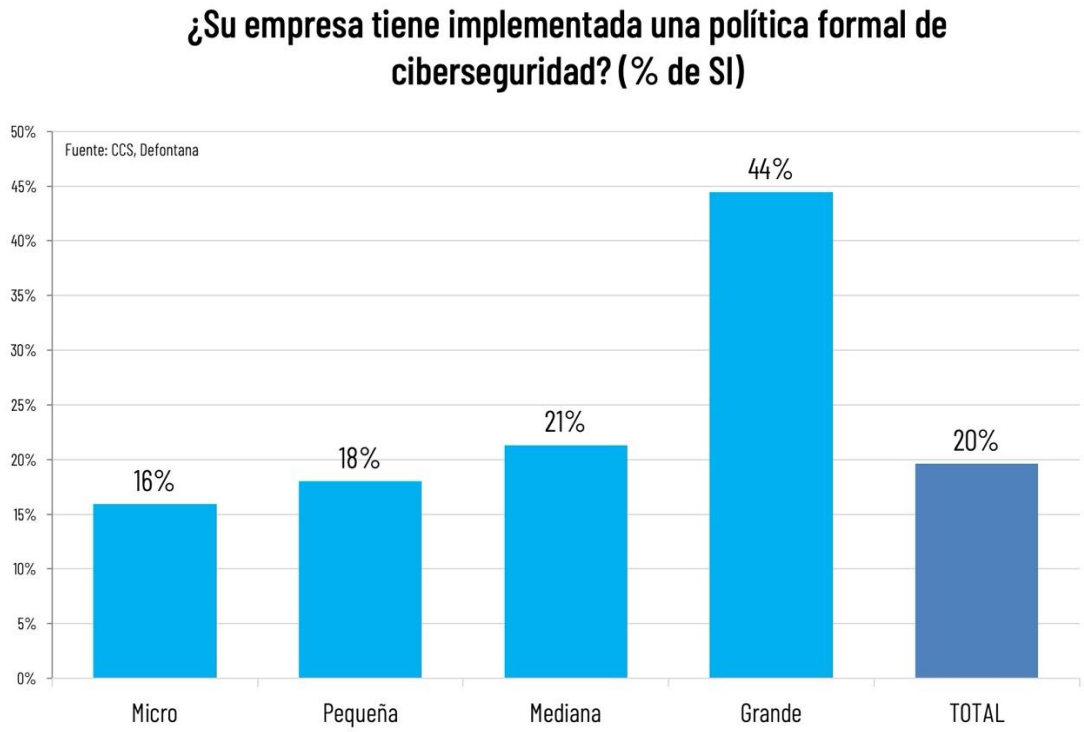


Fuente: CCS, Defontana

Esta distribución sugiere la existencia de dos segmentos empresariales diferenciados: uno proactivo que reconoce la urgencia del tema y otro que subestima los riesgos asociados o enfrenta restricciones de recursos que postergan la implementación.

Políticas formales de ciberseguridad

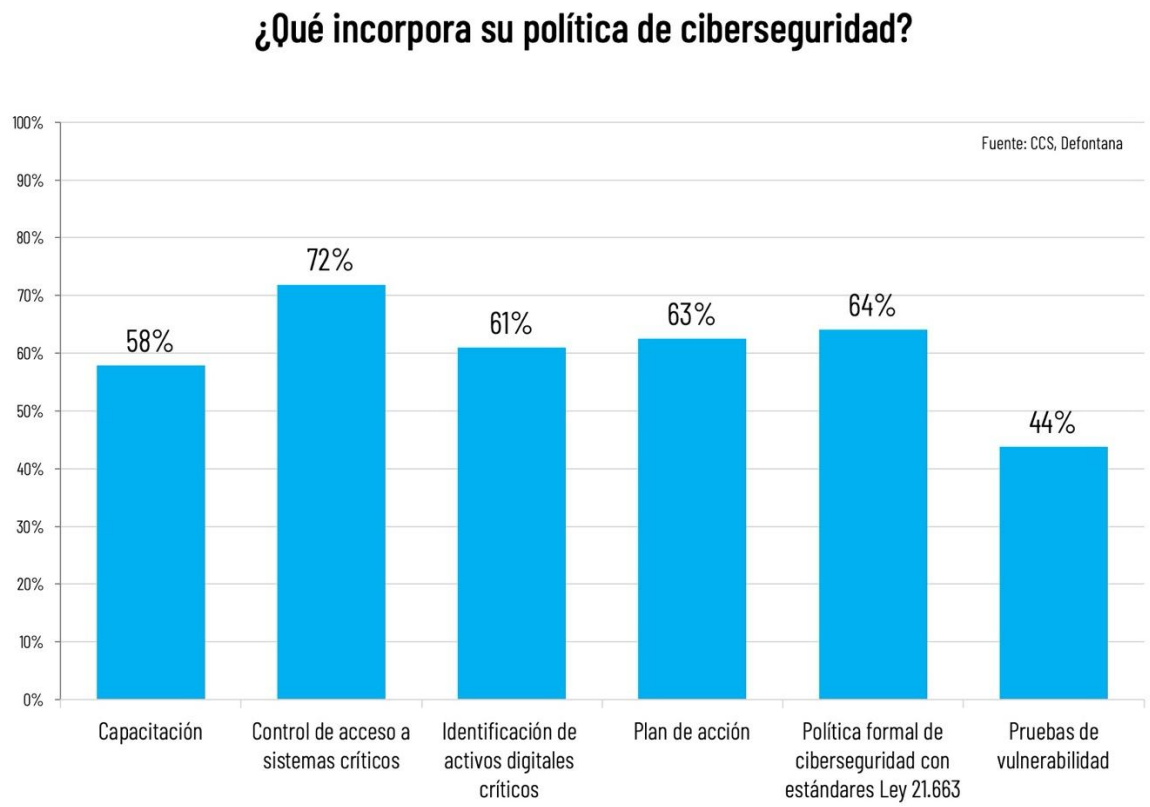
Los resultados evidencian una implementación notablemente baja en la mayoría de los estratos empresariales, con un promedio general del 20%. Las grandes empresas lideran con 44%, mientras que las microempresas presentan apenas 16% de implementación, las pequeñas del 18% y las medianas del 21%. En otras palabras, más de la mitad de las grandes empresas (56%) y la vasta mayoría de las pymes (80-85%), carecen actualmente de una política de ciberseguridad.



La baja penetración general de políticas de ciberseguridad revela una posible vulnerabilidad sistémica en el ecosistema empresarial chileno. Esta situación puede generar externalidades negativas considerables, donde los riesgos en empresas menores pueden comprometer la seguridad de cadenas de valor completas.

Esta escasa penetración de políticas formales sugiere que la gestión de la ciberseguridad aún no ha sido institucionalizada en muchas organizaciones, quedando posiblemente relegada a medidas informales o reactivas. Dado el auge de amenazas cibernéticas (fraudes electrónicos, robos de datos, ransomware) y la potencial exposición financiera y reputacional asociada, la ausencia de políticas estructuradas representa un riesgo latente para la continuidad de negocio, especialmente en las pymes que tienden a ser más vulnerables.

Las implicancias económicas de esta brecha son significativas: inversiones en ciberseguridad y cumplimiento podrían traducirse en mayor resiliencia y menor costo por incidentes en el mediano plazo, por lo que fomentar políticas formales en empresas de todos los tamaños resulta prioritario para elevar el nivel de preparación del sector privado frente a riesgos digitales.



Componentes de las políticas de ciberseguridad

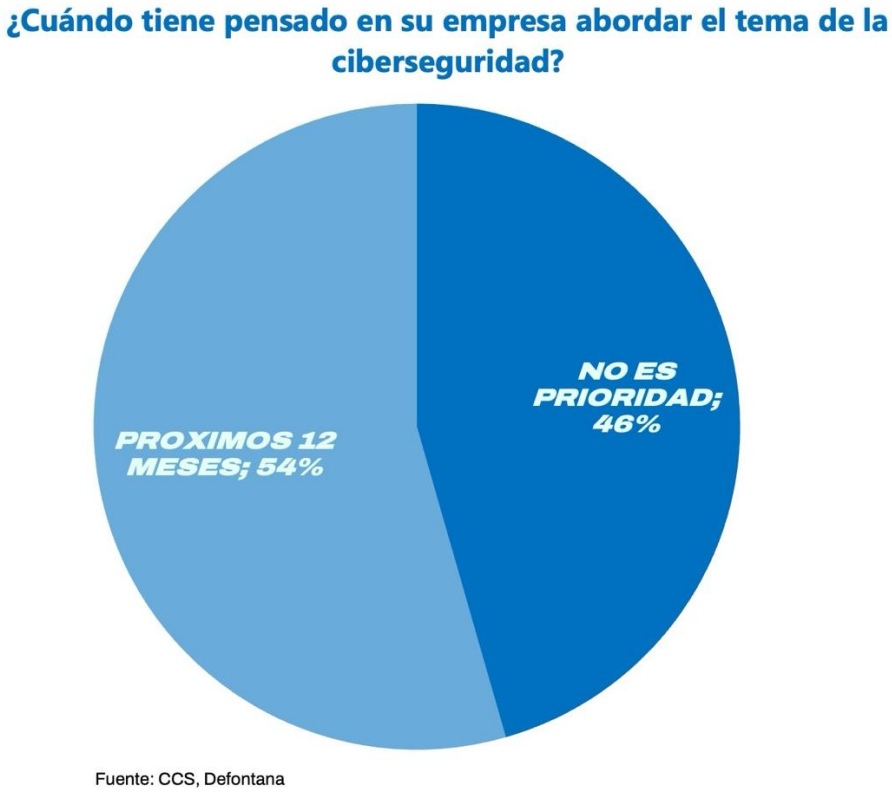
El control de acceso a sistemas críticos emerge como el componente más prevalente (72%), seguido por políticas formales alineadas con la Ley 21.663 (64%), y planes de acción (63%). La capacitación presenta un nivel intermedio (58%), mientras que las pruebas de vulnerabilidad muestran la menor implementación (44%)

Esta distribución indica un enfoque centrado en medidas de control de acceso inmediatas, con menor énfasis en elementos proactivos, como testing de vulnerabilidades.

En suma, las políticas de ciberseguridad vigentes tienden a cubrir los aspectos básicos de capacitación y control de accesos, y en buena medida buscan alinearse con el nuevo marco normativo, pero parecen adolecer de profundidad en herramientas avanzadas de gestión de riesgos (como planificación de respuesta y testeos). Esto podría indicar una madurez incipiente en los programas de seguridad: muchas empresas han dado pasos iniciales (establecer políticas, normas de acceso, etc.), pero aún no incorporan plenamente el ciclo de mejora continua que implican los ejercicios de simulación y la formulación de planes detallados de respuesta ante incidentes.

Fortalecer estos componentes menos adoptados sería crucial para que las políticas existentes pasen de un enfoque principalmente preventivo estático (establecer reglas) a uno dinámico y resiliente, donde la preparación y la evaluación continua reduzcan efectivamente la probabilidad e impacto de los eventos de ciberseguridad.

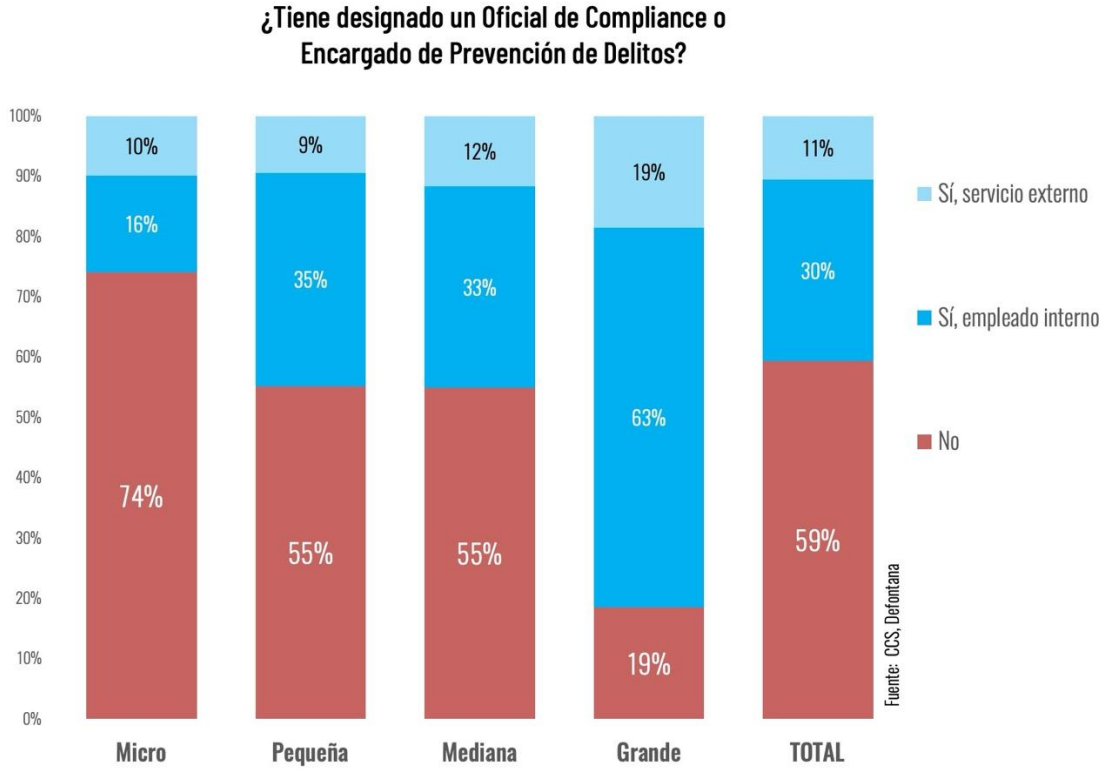
Los datos muestran una ligera inclinación hacia la implementación futura, con 54% planificando abordar ciberseguridad en los próximos 12 meses y 46% sin considerarlo prioritario



Fuente: CCS, Defontana

Designación de oficiales de compliance

Los resultados revelan que 59% de las empresas carecen de oficiales de compliance designados. Entre las que sí cuentan con esta función, predominan los servicios externos (30%), sobre empleados internos (11%). Las grandes empresas muestran un patrón inverso, con 63% utilizando servicios externos y 19% empleados internos, mientras que un 74% de las microempresas carecen completamente de esta función.



La alta prevalencia de servicios externos sugiere la existencia de economías de escala en servicios especializados de compliance. Para empresas grandes, la externalización puede representar acceso a expertise especializado, mientras que para empresas menores constituye la única opción viable económicamente.

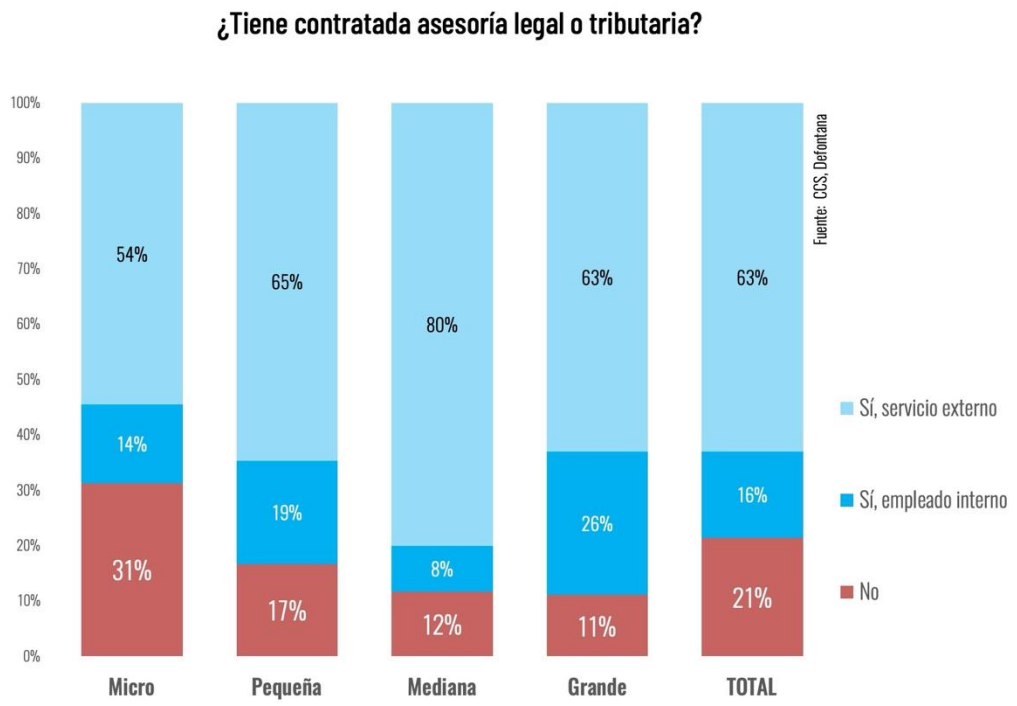
las organizaciones de mayor tamaño no solo implementan más modelos y políticas, sino que también designan responsables claros para gestionarlos, lo que probablemente redunda en un cumplimiento más efectivo. En cambio, la ausencia de un oficial en empresas pequeñas puede implicar un menor seguimiento de las materias de cumplimiento en el día a día. Desde una perspectiva institucional, resulta clave promover mecanismos para que las pymes accedan a servicios de compliance asequibles (por ejemplo, asesorías compartidas o figuras asociativas), de modo que ninguna empresa quede sin acceso a orientación experta. A medida que el entorno regulatorio se torna más exigente, la profesionalización de la función de cumplimiento será un factor diferenciador para evitar sanciones y mejorar las prácticas éticas en empresas de todo porte.

Contratación de asesoría legal o tributaria

Finalmente, el informe examina en qué medida las empresas cuentan con asesoría legal o tributaria externa o interna de forma permanente, lo cual es indicativo de su capacidad para manejar temas complejos de normativa, impuestos y contratos.

Los resultados muestran nuevamente un patrón de relación directa entre tamaño de empresa y uso de asesoría especializada. Las microempresas presentan el menor penetración, con un 54% de ellas utilizando servicios externos y un 14% capacidades internas, mientras que casi un tercio declara no contar con este tipo de servicios. Esta última proporción disminuye a un 17% en las pequeñas empresas, un 12% en las medianas y un 11% en las grandes.

Estos resultados sugieren que el segmento micro suele apoyarse en gestión propia o empírica para sus obligaciones legales y fiscales, posiblemente por restricciones de presupuesto o porque percibe sus operaciones como simples. Sin embargo, implica también un riesgo de desconocimiento normativo o errores en el cumplimiento tributario por falta de guía especializada.



A medida que aumenta el tamaño empresarial, crece la proporción que dispone de asesoría. En las pequeñas empresas, si bien predomina aún la ausencia de consejo jurídico permanente, ya es más común contratar asesores externos, e incluso algunas cuentan con personal interno encargado de asuntos legales o tributarios. En las empresas medianas, la presencia de apoyo legal/tributario aumenta a un 88%. Por último, en las grandes empresas la institucionalización de departamentos legales y contables es la norma: una alta proporción dispone de equipos jurídicos o tributarios propios, complementados en ciertos casos por consultores externos para materias especializadas.

En general, los resultados de este primer diagnóstico revelan un panorama heterogéneo del compliance empresarial en Chile, caracterizado por significativas brechas entre conocimiento normativo e implementación efectiva, así como marcadas asimetrías según el tamaño empresarial. La evidencia sugiere la necesidad de un trabajo diferenciado que aborde las restricciones específicas de cada segmento empresarial, particularmente en áreas emergentes como ciberseguridad, donde la vulnerabilidad sistémica requiere de una intervención coordinada.