LITORALPRESS

Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: Un equipo preparado para apoyar a las empresas frente a los desafíos de la Ley Marco de Ciberseguridad

Pág. : 22
Cm2: 557,4

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

César Pallavicini Z. CEO; **Pietro Pallavicini Z.** Gerente de Proyectos, **Luis Burgos B.** Abogado/consultor y **Cristian Aguayo M.** Gerente de Consultoría.

Pallavicini Consultores

Un equipo preparado para apoyar a las empresas frente a los desafíos de la Ley Marco de Ciberseguridad

La Ley N° 21.663 marca un antes y un después en la manera en que las organizaciones enfrentan la ciberseguridad en Chile. Más allá de exigencias técnicas, establece deberes concretos de reporte, gobernanza y gestión. En esta entrevista, cuatro expertos de Pallavicini, consultora boutique especializada en ciberseguridad, analizan los principales desafíos que plantea su cumplimiento y entregan una hoja de ruta para avanzar.

¿Por qué el deber de reporte se ha convertido en una obligación clave para las organizaciones sujetas a la Ley 21.663?

Luis Burgos: Porque es la obligación más concreta e inmediata para las entidades calificadas como prestadores de servicios esenciales o como operadores de importancia vital. La ley exige reportar incidentes de ciberseguridad dentro de un plazo de tres horas desde que se detecte un efecto significativo, según los artículos 9° y 27°. Pero no basta con lo técnico: el proceso de reporte exige gobernanza. La entidad debe tener protocolos de escalamiento, criterios de impacto, responsables designados y documentación que respalde las decisiones. Incluso, si se concluye que un incidente no es reportable, debe existir trazabilidad. El objetivo es que las organizaciones no solo reaccionen, sino que demuestren una capacidad efectiva de gestión ante amenazas digitales.

¿Están las empresas preparadas para dar cumplimiento a la Ley Marco de Ciberseguridad?

César Pallavicini: Si bien las grandes organizaciones reguladas o multinacionales han mejorado en riesgo operacional, muchas otras siguen al debe. Aún es común la ausencia de un Oficial de Seguridad de la Información (CISO), de un comité de seguridad que sesione regularmente, o de políticas y procedimientos documentados. Además, no existen protocolos formales para responder a situaciones como una ciberextorsión, y en muchos casos los planes de continuidad del negocio están desactualizados. Esto impide una rápida recuperación de los procesos de negocio y una respuesta eficaz frente a eventos críticos. Según cifras, menos de 300 empresas en Chile cuentan con la certificación ISO 27001:2022, lo que evidencia una brecha importante en términos de preparación.

¿Qué rol cumple un SGSI ISO 27001 en el cumplimiento de esta Ley?

Pietro Pallavicini: Desarrollar un Sistema de Gestión de Seguridad de la Infor-

LITORALPRESS

Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: Un equipo preparado para apoyar a las empresas frente a los desafíos de la Ley Marco de Ciberseguridad

Pág. : 23
Cm2: 283,0

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

mación (SGSI) basado en ISO 27001 es clave para cumplir con la esta Ley Marco, ya que entrega las mejores prácticas y representa un desde , respecto a la ley antes mencionada.

Asimismo, contar con un SGSI certificable otorga una ventaja estratégica: genera confianza entre los stakeholders y fortalece la posición competitiva de la empresa. El SGSI, junto a los controles definidos en la ISO 27002, facilita la preparación y respuesta ante incidentes, además de ordenar la comunicación con las autoridades competentes.

¿La certificación ISO 27001:2022 resuelve por completo las exigencias de la ley?

César Pallavicini: No, pero es un paso fundamental para avanzar. ISO 27001:2022 se complementa con otros marcos como ISO 27032 (controles específicos de ciberseguridad), el NIST CSF y la norma ISO 27701, enfocada en la gestión de la privacidad. Esta última es aún poco conocida en Chile, pero también certificable, y muy útil para abordar aspectos de protección de datos personales.

¿Qué pasos concretos recomiendan para comenzar a cumplir con la ley?

Cristian Aguayo: Frente a un marco legal cada vez más exigente, las organizaciones deben adoptar un enfoque estructurado y proactivo. A continuación, detallo cinco pasos esenciales para avanzar de manera concreta en el cumplimiento de la Ley Marco de Ciberseguridad:

Diagnóstico inicial de madurez: Evaluar la situación actual en ciberseguridad, identificando brechas frente a estándares como ISO 27001, 27032 y NIST CSF.

Inventario de activos críticos: Identificar procesos, servicios o tecnologías cuya afectación impacte la continuidad operativa.

Gestión de incidentes: Diseñar un proceso formal, probado, entrenado y revisado al menos una vez al año.

Gobernanza del reporte: Definir quién decide, quién reporta y cómo se documentan las decisiones. Debe involucrar a la alta dirección y asegurar formalidad ante ANCI y otros reguladores.

Capacitación y simulacros: Tener documentos no basta. Hay que entrenar a los equipos y simular incidentes reales para mejorar tiempos de reacción y validar roles y protocolos.

Este proceso debe incluir un playbook institucional: políticas formales, procedimientos claros, protocolos de escalamiento, criterios de decisión y responsables definidos. La participación activa de la alta dirección es clave, evaluando no solo el cumplimiento normativo, sino también el impacto en la continuidad del negocio y la reputación de la organización.