ELECTRO INDUSTRIA
Soluciones Tecnológicas para la Minería, Energía e Industria

Fecha: 31/07/2025 Audiencia: 0 Sección: ESPECIALES
Vpe: $595.845 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $661.122 Difusión: 0
Vpe portada: $661.122 Ocupación: 90,13%

CSIRTs empresariales

Claves para cumplir con la Ley Marco de Ciberseguridad en Chile

Con foco en la implementación efectiva de CSIRTs empresariales, el seminario "Exigencias y oportunidades en la gestión de incidentes de ciberseguridad en Chile" abordó los desafíos técnicos, normativos y organizacionales que impone la nueva Ley Marco de Ciberseguridad, marcando un hito en la articulación público-privada para la respuesta ante incidentes en nuestro país.

En junio pasado, se celebró con una convocatoria récord tanto presencial como virtual, el seminario "Exigencias y oportunidades en la gestión de incidentes de ciberseguridad en Chile", organizado por la Alianza Chilena de Ciberseguridad (ACC), Business Continuity, COPEC y la Asociación de Transmisoras de Chile. El evento congregó a líderes sectoriales, técnicos, jurídicos y estratégicos para abordar la aplicación de la Ley Marco de Ciberseguridad (Ley 21.663), así como el avance en la construcción de capacidades organizacionales para responder a incidentes, principalmente a través de la formalización de CSIRTs en las empresas.

Realizada en las instalaciones de Copec, la jornada fue ampliamente valorada por su enfoque técnico, estratégico y colaborativo. En ese sentido, las intervenciones demostraron que los actores clave del ecosistema digital chileno reconocen la urgencia de avanzar hacia una institucionalización efectiva de los CSIRTs (sigla en inglés de "Equipo de Respuesta ante Incidentes de Seguridad Informática"), entendidos como órganos responsables de coordinar la respuesta ante incidentes y cumplir con las exigencias regulatorias de notificación, trazabilidad y articulación sectorial.

Visión estratégica desde la ANCI

El Director de la Agencia Nacional de Ciberseguridad (ANCI), Daniel Álvarez, dio apertura al seminario enfatizando el rol protagónico de los CSIRTs en la gestión de incidentes y el cumplimiento regulatorio. Recalcó que dichos equipos deberán estructurarse formalmente al interior de las organizaciones, ser operativos y funcionar bajo un marco de gobernanza claro. También subrayó que la Ley Marco además de plantear

(Continúa en página 32)

ELECTRO INDUSTRIA
Soluciones Tecnológicas para la Minería, Energía e Industria
Fecha: 31/07/2025 Audiencia: 0 Sección: ESPECIALES
Vpe: $590.863 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $661.122 Difusión: 0
Vpe portada: $661.122 Ocupación: 89,37%

(Viene de página 30)

"La ciberseguridad es ahora un componente central de la continuidad operacional. Las empresas deben contar con un órgano que sepa reaccionar, notificar, escalar y coordinar"

obligaciones, habilita espacios de colaboración público-privada para el fortalecimiento institucional.
Álvarez llamó a las organizaciones a entender que los CSIRTs son una necesidad transversal, no exclusiva de las áreas técnicas: "La ciberseguridad es ahora un componente central de la continuidad operacional. Las empresas deben contar con un órgano que sepa reaccionar, notificar, escalar y coordinar. El cumplimiento no puede quedarse en el papel; debe expresarse en capacidades concretas".

Liderazgo regional con responsabilidad institucional

Posteriormente, el Senador Kenneth Pugh reforzó el mensaje político y estratégico del seminario, señalando que Chile, al promulgar tempranamente su Ley Marco de Ciberseguridad, se posicionó como líder normativo en la Región.
Sin embargo, advirtió que dicho liderazgo implica responsabilidad técnica. "La ley nos posiciona internacionalmente, pero ahora corresponde demostrar capacidad operativa, compromiso institucional y articulación multisectorial. Nadie se puede quedar atrás", agregó.

Experiencias empresariales y multidisciplinariedad aplicada

El panel del conversatorio, moderado por Carlos Vera Gómez (CISO de SerCor y líder de la Plataforma Estratégica de Ciberseguridad de la ACC), reunió a representantes de empresas e instituciones que compartieron experiencias sobre el diseño, estructuración y operación de CSIRTs. En esta ocasión, participaron:

- Katherina Canales Madrid, COO de Aura Cybersecurity, quien destacó la importancia de integrar a mujeres en liderazgo técnico en CSIRTs.
- Luis Felipe Espinoza, Sub-Gerente de Ciberseguridad en Copec, quien compartió desafíos del sector energético en la protección de entornos críticos.
- Carlos Figueroa, Director de la Asociación de Transmisoras de Chile AG, que enfatizó la necesidad de coordinación sectorial para lograr eficiencia operativa.
- Ricardo Urbina, CISO del Grupo Elecmetal, quien abordó la implementación progresiva en entornos industriales.
- Jorge Olivares, Gerente de Consultoría y Formación de Business Continuity, quien presentó modelos metodológicos de CSIRTs adaptados al cumplimiento normativo nacional.

El panel coincidió en que los CSIRTs deben ser equipos institucionalizados, con presupuesto, personal capacitado y respaldo estratégico. Además, se remarcó la necesidad de que estos equipos sean interdisciplinarios, integrando expertos técnicos, legales, de gestión y comunicación, capaces de actuar coordinadamente ante eventos complejos.
Asimismo, indicó que la Ley Marco exige no solo contar con CSIRTs formales, sino operarlos conforme a buenas prácticas internacionales. En ese sentido, se mencionó marcos como ISO/IEC 27035, NIST SP 800-61, NERC-CIP, y COBIT 2019.
También se valoró que Chile cuente con marcos nacionales claros, como la propia Ley 21.663, que exige notificación obligatoria de incidentes y formalización de capacidades operativas. La clave está ahora en convertir esas exigencias normativas en capacidades efectivas dentro de cada organización.

Hacia una arquitectura federada de CSIRTs

De igual modo, se propuso avanzar hacia una arquitectura federada de CSIRTs, articulando:

- Equipos internos en cada organización que operen de forma especializada.
- CSIRTs sectoriales impulsados por gremios y asociaciones.
- Coordinación nacional liderada por el CSIRT Nacional y supervisada por la ANCI.

Esta estructura mejora la trazabilidad, la coordinación intersectorial y la respuesta ante incidentes sistémicos. La federación permite avanzar sin duplicar esfuerzos, utilizando capacidades existentes, y definiendo responsabilidades claras.
Para Luis Felipe Espinoza, SubGerente de Ciberseguridad de Copec, un

(Continúa en página 34)

ELECTRO INDUSTRIA
Soluciones Tecnológicas para la Minería, Energía e Industria
Fecha: 31/07/2025 Audiencia: 0 Sección: ESPECIALES
Vpe: $563.961 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $661.122 Difusión: 0
Vpe portada: $661.122 Ocupación: 85,3%

(Viene de página 32)

ciberataque a una empresa ya no es un problema aislado. "Es un desafío para todo el ecosistema. La nueva ley fomenta precisamente esa cultura de colaboración", afirmó.

Enfoques de implementación

Aunque la formalización de CSIRTs es una exigencia, no se plantea un modelo específico a seguir, y los sugeridos en marcos metodológicos internacionales tienden a considerarse muy extensos, lineales y complejos. En contraposición, se está optando por enfoques evolutivos, que permiten construir capacidades de forma modular y progresiva.

Para Olivares, se propicia el desarrollo de versiones mínimas viables de CSIRTs, que cumplen funciones básicas como el registro, la coordinación y la notificación de incidentes. Luego, estas versiones se enriquecen mediante la incorporación gradual de módulos más especializados, como automatización, análisis forense, monitoreo y simulacros.

"Este enfoque no reemplaza las exigencias legales, pero permite avanzar de manera efectiva en contextos reales. Lo esencial es iniciar el proceso, institucionalizar capacidades, y crecer de forma iterativa, documentada y respaldada por estándares", sostuvo.

Ricardo Urbina, CISO del Grupo Elecmetal, señaló: "Llegó el momento de verificar lo declarado en los procedimientos de gestión de ciberincidentes, considerando las exigencias legales y su capacidad de probarlos, de lo contrario el riesgo de pérdidas en dinero, capacidad productiva y hasta en vidas, podría ser una triste realidad".

Construir CSIRTs es construir resiliencia organizacional

El seminario dejó claro que los CSIRTs empresariales es un paso esencial para cumplir con la Ley Marco de Ciberseguridad, pero también representa una inversión en continuidad operativa, reputación corporativa y resiliencia organizacional. Los CSIRTs reaccionan ante amenazas, coordinan respuesta técnica, escalan situaciones críticas y permiten que las empresas se alineen con los requerimientos regulatorios.

Chile cuenta con un marco legal robusto, con expertos disponibles, y con voluntad institucional. La tarea ahora está en manos de cada empresa, cada sector y cada equipo técnico. Formalizar un CSIRT no es solo cumplir la ley: es declarar que la ciberseguridad importa, que la respuesta ante incidentes está organizada, y que el país avanza hacia un modelo colaborativo, federado y estratégico en materia de protección digital.

Artículo gentileza de Jorge Olivares Olmos,
Gerente de Consultoría y Formación de Business Continuity SpA, y Ex-Instructor Oficial de Carnegie Mellon para CSIRTs.
jorge_olivares@businesscontinuity.cl