Kiteworks

COMPLIANCE BRIEF

Chile's Law 21.663 and How Kiteworks Secures Your Critical Infrastructure

Stay Ahead of Chile's Cybersecurity Law With Encryption, Access Governance, and Audit Compliance

Chile's Law 21.663 on Cybersecurity Framework establishes Chile's national cybersecurity framework with most provisions that became effective January 1, 2025, and key obligations for operators of vital importance, incident reporting, and sanctions that began March 1, 2025. This comprehensive legislation mandates compliance for all government entities at national, regional, and municipal levels, as well as private sector organizations classified as essential service providers spanning critical infrastructure sectors including energy, water, telecommunications, transportation, healthcare, financial services, and digital infrastructure providers. The law applies throughout Chilean territory to organizations providing essential services or classified as operators of vital importance. Importantly, Law 21.663 works alongside Law 21.719 on personal data protection to create an integrated security framework—where cybersecurity infrastructure provides the technical foundation for effective data protection. Noncompliance triggers administrative sanctions under a graduated system: minor violations up to 5,000 Monthly Tax Units (UTM), serious violations up to 10,000 UTM, and very serious violations up to 20,000 UTM, with penalties doubled for operators of vital importance (reaching up to 40,000 UTM), enforced by the newly created National Cybersecurity Agency (ANCI). Kiteworks supports organizations working toward compliance with Law 21.663. Here's how:

Hardened Infrastructure and Encryption Standards

Articles 3, 7, and 8 of Law 21.663 mandate implementing technical security measures and continuous information security management systems to protect network and data confidentiality, integrity, and availability. Article 3 establishes the principle of IT security, affirming every person's right to adopt necessary technical security measures including encryption. These requirements align with Law 21.719's security principle, where cybersecurity measures directly support personal data protection obligations. Violations carry graduated administrative sanctions with penalties doubled for operators of vital importance (especially for Operadores de importancia vital [OIVs] under Article 8). Kiteworks deploys as a hardened virtual appliance with multiple protection layers that minimize attack surface, incorporating an embedded zero-maintenance network firewall blocking all unused ports and an embedded web application firewall with automated rules updates. The platform implements double encryption at rest using AES-256 for both files and disk storage, while TLS 1.2+ protocols secure data in transit.

Solution Highlights

- **Strong double encryption**
- **Zero Trust Mode**
- **Data Policy Engine with ABAC and RBAC**
- **Real-time SIEM integration**
- **Intrusion detection**

Access Governance and Incident Response Controls

The damage control principles in Article 3 require coordinated response to prevent cyberattack escalation, while Article 8 mandates specific duties for operators of vital importance including rapid implementation of measures to reduce incident impact and propagation. Article 8(g) requires operators to inform potentially affected parties about incidents or cyberattacks that could seriously compromise their information or IT systems when requested by ANCI, particularly when involving personal data and no other legal notification duty applies—a requirement that complements Law 21.719's breach notification obligations to the Data Protection Agency. Kiteworks enforces enterprise-grade governance through combined RBAC and ABAC controls aligned to NIST CSF framework standards, with the Data Policy Engine enabling compliance administrators to define dynamic policies based on data attributes, user profiles, and contextual factors. Zero Trust Mode blocks all IP addresses by default except those explicitly allowed, while intrusion detection maintains an evolving pattern library to identify suspicious network activities. The platform automatically notifies administrators of detected threats through real-time console banners and logs all intrusion attempts for security operations teams.

Comprehensive Audit Logging and Reporting Obligations

Article 8(b) mandates maintaining complete records of security management system actions while Article 9 requires reporting significant cybersecurity incidents to the National CSIRT within specific time frames: 3-hour initial alert, 72-hour detailed update (24 hours for vital operators with service disruption), and 15-day final report. When cyber incidents involve personal data breaches, organizations must coordinate dual reporting to both ANCI under Law 21.663 and the Data Protection Agency under Law 21.719. The National CSIRT, established under Article 24, coordinates incident response across government agencies and serves as the national point of contact for international cybersecurity collaboration. Kiteworks captures all user, administrator, and system activities in a unified audit log without throttling or data loss, tracking every file access attempt with complete forensic detail. The platform feeds comprehensive logs in real time to external SIEM systems including Splunk via syslog, enabling immediate incident detection and response coordination. For organizations subject to sector-specific requirements, MFT Client records detailed flow logs for every executed workflow and sends them to associated server clusters. The audit log maps help compliance officers identify location-based risks and demonstrate adherence to Chile's mandatory reporting timelines through automated compliance reports.

Conclusion

Chile's Law 21.663 establishes comprehensive cybersecurity obligations across protection, control, and tracking domains that organizations must address through integrated technical and procedural measures. This cybersecurity framework works in tandem with Law 21.719 on personal data protection, creating a unified approach where strong cybersecurity infrastructure supports data privacy compliance. For protection requirements, Kiteworks deploys hardened infrastructure with double encryption at rest and TLS 1.2+ in transit. For control mandates, the platform enforces RBAC and ABAC governance aligned to NIST CSF standards, implements Zero Trust Mode with default-deny IP blocking, and enables immediate incident response through emergency access revocation and kill switch capabilities. For tracking obligations, Kiteworks captures complete audit logs without throttling, feeds data in realtime to SIEM systems via syslog, and generates automated compliance reports demonstrating adherence to mandatory incident reporting timelines. As organizations face penalties under the graduated sanctions system—ranging from written warnings to 5,000 UTM for minor violations, up to 10,000 UTM for serious violations, and reaching 20,000 UTM for very serious violations (with penalties doubled for operators of vital importance to a maximum of 40,000 UTM under Article 40)—Kiteworks provides a unified platform that addresses all three compliance pillars through a single integrated solution while supporting the complementary data protection requirements of Law 21.719.