ManageEngine

Guía práctica de la Ley Marco de Ciberseguridad en Chile (Ley 21.663)

manageengine.com/latam/

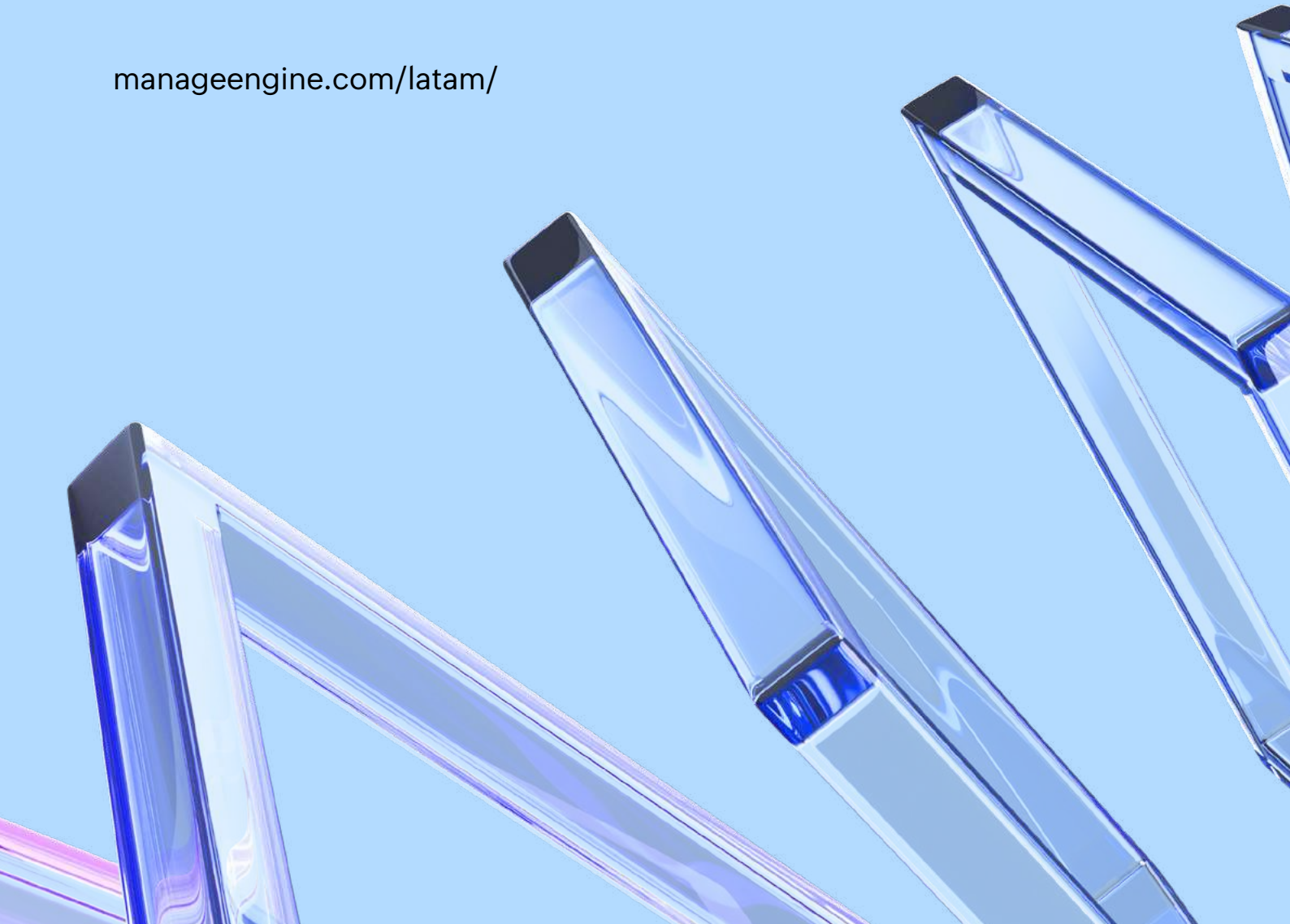


Tabla de contenido

Introducción

En los últimos años, la transformación digital ha acelerado la interconexión de sistemas y servicios en todos los sectores, aumentando significativamente los riesgos cibernéticos. Chile no ha estado ajeno a esta realidad. Con ciberataques dirigidos tanto a instituciones públicas como a empresas privadas, la necesidad de contar con un marco legal robusto y moderno se volvió urgente.

La Ley Marco de Ciberseguridad (Ley 21.663), representa un hito en la legislación chilena. Esta normativa busca fortalecer la seguridad de la información y la protección de los sistemas críticos del país, alineándose con estándares internacionales y promoviendo una cultura de prevención frente a las amenazas digitales.

Este ebook te permitirá conocer de manera clara, práctica y accesible los aspectos más relevantes de esta nueva ley, sus implicaciones y cómo prepararte para cumplir con sus exigencias.

¿Qué es la Ley 21.663?

La Ley 21.663, conocida como la Ley Marco de Ciberseguridad, es la primera legislación integral en Chile enfocada exclusivamente en establecer un sistema nacional para la prevención, detección, respuesta y recuperación ante incidentes de ciberseguridad.

Promulgada el 26 de marzo de 2024, tiene como objetivo “establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre estos y los particulares”.

Esta Ley, que entró en vigencia el 1 de marzo de 2025, establece principios, obligaciones y responsabilidades para entidades públicas y privadas que gestionen Infraestructura Crítica de la Información (ICI).

Además, crea un nuevo ecosistema institucional liderado por la Agencia Nacional de Ciberseguridad (ANCI), convirtiéndo a Chile en el primer país de Latinoamérica y el Caribe en tener una agencia de este tipo.

Este marco es un modelo de cooperación entre el sector público y privado, que regula aspectos como la notificación obligatoria de incidentes, la gobernanza de los sistemas informáticos y un régimen sancionatorio en caso de incumplimientos.

Objetivos principales

- Proteger la infraestructura crítica digital del país.
- Fortalecer la capacidad de respuesta ante ciberamenazas.
- Establecer reglas claras sobre responsabilidades y coordinación.
- Promover la colaboración entre el sector público, privado y la ciudadanía.

¿A quién aplica?

Esta Ley aplica a organismos del Estado, incluyendo ministerios, servicios públicos, municipios y empresas públicas.

Entidades privadas que presten servicios esenciales o críticos, tales como:

- Empresas de telecomunicaciones
- Proveedores de servicios financieros
- Empresas de energía, agua potable y transporte
- Organizaciones de salud
- Infraestructura digital crítica (como centros de datos, redes o servicios cloud)
- Empresas de transporte y logística crítica.
- Plataformas tecnológicas que administren datos sensibles o de alto valor estratégico.

Estas empresas pueden ser designadas formalmente como “sujetos obligados” por la ANCI, lo que activa una serie de responsabilidades.

Cualquier entidad pública o privada que administre o controle sistemas considerados como infraestructura crítica de la información (ICI) entra en el marco de esta ley.

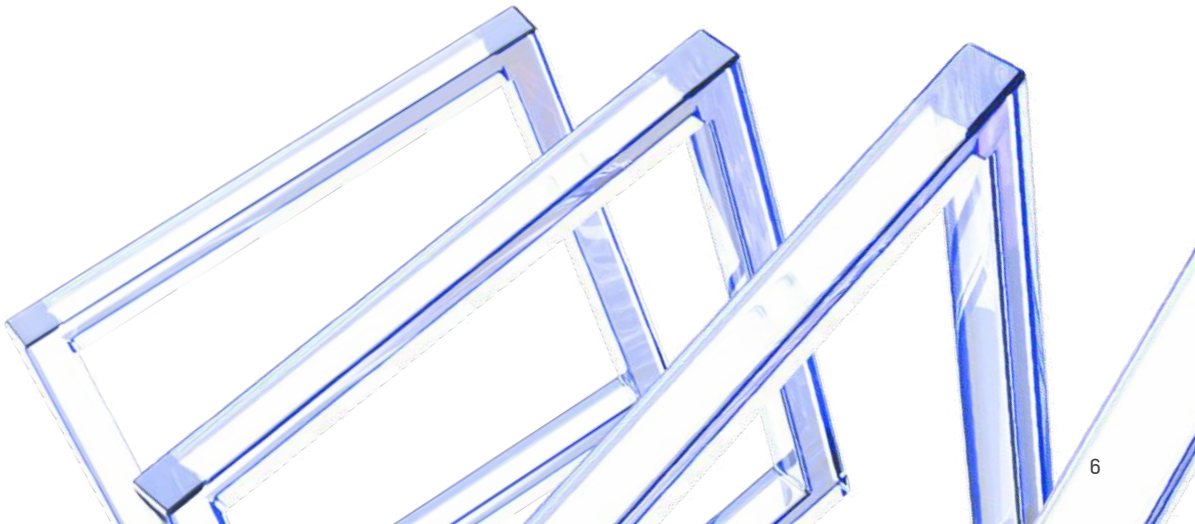
Definiciones clave

Infraestructura Crítica de la Información (ICI): sistemas cuya afectación, interrupción o destrucción puede generar consecuencias graves para la seguridad nacional, el orden público o el bienestar de la ciudadanía.

Ciberincidente: cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de los sistemas informáticos o la información contenida en ellos.

Sistema de gestión de la ciberseguridad: conjunto de políticas, procedimientos y tecnologías implementadas por una organización para prevenir, detectar y responder a amenazas cibernéticas.

Sujetos obligados: entidades determinadas por la ley que deben cumplir con obligaciones específicas como notificación de incidentes, implementación de medidas de protección y auditorías.



Institucionalidad: nuevas estructuras para enfrentar amenazas cibernéticas

Uno de los pilares de la Ley 21.663 es la creación de un sistema de gobernanza clara y coordinada para la ciberseguridad en Chile. Esto incluye la consolidación de instituciones existentes y la creación de nuevos organismos especializados.

Agencia Nacional de Ciberseguridad (ANCI)

La ANCI es el organismo central del nuevo sistema nacional de ciberseguridad. Fue creada con el propósito de coordinar, supervisar y fiscalizar el cumplimiento de la ley.

Funciones principales de la ANCI:

- Supervisar el cumplimiento de las obligaciones de ciberseguridad en entidades públicas y privadas.
- Determinar y actualizar el listado de infraestructuras críticas de la información.
- Exigir la notificación de incidentes de ciberseguridad.
- Emitir directrices, estándares y normativas técnicas.
- Aplicar sanciones por infracciones a la ley.
- Coordinarse con organismos internacionales en materia de ciberseguridad.

CSIRT Nacional (Equipo de Respuesta ante Incidentes de Seguridad Informática)

El CSIRT Nacional, dependiente de la ANCI, cumple un rol técnico-operativo y de respuesta ante incidentes.

Sus funciones incluyen:

- Monitorear y analizar amenazas a nivel nacional.
- Apoyar a los sujetos obligados en la detección y gestión de incidentes.
- Emitir alertas tempranas y reportes de seguridad.
- Promover la colaboración público-privada en ciberdefensa.
- Prestar asistencia técnica a las instituciones afectadas.

El CSIRT actúa como el "primer respondiente" en caso de ciberataques que puedan afectar la infraestructura crítica nacional o generar un impacto significativo en los servicios esenciales.

Coordinación y colaboración

Además de la ANCI y el CSIRT, la ley establece mecanismos para que otros actores del Estado, como el Ministerio del Interior, el Ministerio de Defensa y los reguladores sectoriales, colaboren activamente en el ecosistema nacional de ciberseguridad.

Lo anterior, con el objetivo de crear un ecosistema coordinado, donde cada actor asuma su rol frente a la protección de la infraestructura crítica y la respuesta ante eventos que puedan afectar la continuidad operacional, el orden público o la seguridad nacional.

Obligaciones para los organismos sujetos a la ley

La Ley 21.663 impone una serie de obligaciones específicas para los organismos públicos y entidades privadas que administran infraestructura crítica de la información. Estas medidas buscan garantizar la prevención, detección, gestión y respuesta ante incidentes de ciberseguridad.

1. Implementación de medidas técnicas y organizativas

Los organismos obligados deben implementar un sistema de gestión de ciberseguridad, que contemple:

- Políticas de seguridad de la información
- Evaluaciones periódicas de riesgos
- Controles técnicos y operativos
- Gestión de vulnerabilidades
- Protección de la cadena de suministro digital
- Estas medidas deben adecuarse a la criticidad de los servicios que presta cada entidad.

2. Notificación de incidentes

Una de las obligaciones centrales es la notificación obligatoria de incidentes de ciberseguridad al CSIRT Nacional.

Ten en cuenta que:

- Los incidentes deben notificarse dentro de 24 horas desde su detección.
- La notificación debe incluir información detallada sobre el incidente, su posible impacto y las medidas adoptadas.
- En caso de incidentes graves, también puede activarse la coordinación con la Agencia Nacional de Ciberseguridad.

3. Planes de continuidad y recuperación

Las entidades deben contar con planes documentados y actualizados que permitan:

- Asegurar la continuidad operativa ante eventos disruptivos
- Restaurar los servicios de manera segura y ordenada
- Evaluar los daños y evitar que el incidente se repita

4. Auditorías y monitoreo

Las entidades estarán sujetas a auditorías técnicas periódicas. La ANCI podrá exigir informes, revisar evidencias y aplicar sanciones en caso de incumplimiento.

También podrán establecerse auditorías independientes o del regulador sectorial, según el caso.

5. Capacitación y concientización

Todas las organizaciones deben capacitar regularmente a su personal en materia de ciberseguridad, buenas prácticas, manejo de incidentes y uso seguro de los sistemas de información.

Estas obligaciones son clave para fomentar una cultura de ciberseguridad preventiva y para asegurar que las compañías estén preparadas frente a amenazas cada vez más complejas.

Recuerda que un equipo informado es tu primera línea de defensa.

6. Régimen sancionatorio

Para asegurar el cumplimiento efectivo de esta Ley, se establece un régimen sancionatorio claro y progresivo. Esto significa que las organizaciones que no implementen las medidas exigidas o que incumplan sus obligaciones estarán sujetas a sanciones proporcionales a la gravedad de la infracción.

Tipos de infracciones

Las infracciones se clasifican en tres categorías:

Leves

Ejemplo: no entregar información requerida por la ANCI en los plazos estipulados.

Graves

Ejemplo: no notificar un incidente de ciberseguridad que afecte la disponibilidad de servicios esenciales.

Gravísimas

Ejemplo: incumplimiento reiterado de medidas de seguridad que genere un ciberataque con consecuencias críticas para el país.

Multas y sanciones (Artículo 40)

Las multas varían según la clasificación de la infracción:

- Leves: entre 5.000 hasta 10.000 Unidades Tributarias Mensuales (UTM)
- Graves: entre 10.000 hasta 20.000 UTM
- Gravísimas: entre 20.000 hasta 40.000 UTM

En casos extremos, la ANCI podrá:

- Ordenar la suspensión temporal de servicios
- Publicar la infracción para efectos de transparencia
- Informar al Ministerio Público si detecta posibles delitos

7. Principales implicaciones

Aunque en un principio la Ley 21.663 podría parecer dirigida principalmente al sector público, sus disposiciones también tienen un impacto directo en las empresas privadas, especialmente aquellas que operan servicios esenciales o infraestructura crítica de información.

Estas implicaciones podrían ser:

- **Fortalecimiento de la seguridad interna:** las empresas deben implementar sistemas formales de gestión de ciberseguridad, con políticas, procedimientos y controles alineados con estándares internacionales.

- **Inversión en tecnología y talento:** será clave aumentar la inversión en herramientas de detección de amenazas, automatización de respuestas, auditoría continua, y capacitación de personal.

- **Notificación obligatoria de incidentes:** ya no basta con resolver incidentes internamente. Si se produce una afectación significativa, debe ser reportada al CSIRT Nacional dentro de las 24 horas siguientes a su detección.

- **Responsabilidad legal y reputacional:** el incumplimiento puede derivar en multas millonarias y daño a la imagen corporativa, especialmente si el incidente afecta a usuarios o datos personales.

- **Mayor relación con el Estado:** habrá una interacción más frecuente con la ANCI y otras entidades públicas, ya sea para auditorías, consultas técnicas o colaboración en incidentes.

- **Oportunidad para liderar:** aunque representa un desafío, esta ley también es una oportunidad para el sector privado de reforzar su confianza, resiliencia y competitividad, destacando aquellas empresas que demuestren madurez en ciberseguridad frente a clientes, inversionistas y el mercado.

Recomendaciones para prepararse y cumplir con la Ley

La entrada en vigor de esta Ley implica cambios relevantes en cómo las organizaciones abordan la gestión de riesgos digitales. A continuación, te dejamos una guía práctica con pasos clave para asegurar el cumplimiento y fortalecer la postura de ciberseguridad de tu organización.

1. Diagnóstico inicial

Evalúa el estado actual de tu seguridad digital:

- ¿Tienes políticas de ciberseguridad vigentes?
- ¿Conoces tus activos críticos?
- ¿Cuentas con herramientas para prevenir, detectar y responder a incidentes?

Un diagnóstico consciente es el primer paso para identificar brechas y definir prioridades.

2. Implementa un sistema de gestión de ciberseguridad (SGC)

Crea o adapta tu modelo de gestión para que integre:

- Análisis de riesgos periódicos
- Controles técnicos y organizativos
- Protocolos de monitoreo y respuesta
- Gestión de proveedores y terceros
- Ciclos de mejora continua

Idealmente, alinéate con marcos internacionales como ISO 27001 o el **NIST Cybersecurity Framework**.

3. Establece canales de notificación de incidentes

Diseña procesos internos claros para:

- Detectar ciberincidentes rápidamente
- Escalar a los responsables adecuados
- Notificar al CSIRT Nacional dentro de las 24 horas
- Registrar y documentar las acciones tomadas

Esto es clave para cumplir con la ley y reducir el impacto de un ataque.

4. Establece una cultura de seguridad transversal

Promueve una visión organizacional donde la ciberseguridad:

- Sea parte del gobierno corporativo
- Cuente con apoyo de la alta dirección
- Se incorpore en los proyectos desde el diseño (“security by design”)

5. Asóciate con expertos

Contar con aliados tecnológicos o consultores especializados puede ayudarte a:

- Acelerar el cumplimiento regulatorio
- Incorporar herramientas avanzadas (como SIEM, EDR, SOC-as-a-Service)
- Responder mejor ante amenazas emergentes

ManageEngine: el mejor aliado para cumplir con la Ley 21.663

Cumplir con los requisitos de esta Ley no solo implica entender la legislación, sino también contar con las herramientas adecuadas para implementarla de forma efectiva.

ManageEngine ofrece un portafolio robusto de soluciones tecnológicas que permiten a las organizaciones fortalecer su postura de ciberseguridad, automatizar procesos clave y garantizar el cumplimiento normativo.

A continuación, te presentamos cómo cada una de estas soluciones puede ayudarte a abordar distintos aspectos exigidos por la ley.

Artículo 7: deberes generales

La Ley Marco de Ciberseguridad establece que todas las instituciones sujetas a su alcance deben implementar de forma continua y permanente medidas para prevenir, detectar, reportar y resolver incidentes de ciberseguridad. Estas medidas deben abarcar ámbitos tecnológicos, organizacionales, físicos e informativos, y estar alineadas con los protocolos, estándares y lineamientos emitidos por la Agencia Nacional de Ciberseguridad (ANCI) y las autoridades sectoriales correspondientes.

El objetivo central es asegurar una gestión efectiva del riesgo, así como mitigar el impacto de los incidentes sobre la continuidad operativa, la confidencialidad, la integridad y la disponibilidad de la información y los sistemas críticos.

¿Cómo puede ayudar ManageEngine?

Para apoyar el cumplimiento de estos deberes generales, ManageEngine ofrece un conjunto de soluciones diseñadas para fortalecer la ciberresiliencia organizacional:

Log360 (SIEM) - Supervisión y respuesta ante Incidentes

- **Detección instantánea de amenazas:** Log360 utiliza técnicas avanzadas como la correlación de logs de eventos, análisis de fuentes contra amenazas y aprendizaje automático para identificar amenazas internas y externas.

- **Mitigación de ataques:** automatiza la respuesta ante incidentes mediante flujos de trabajo sincronizados con alertas, integrándose con soluciones ITSM para garantizar la resolución efectiva de incidentes.

- **Monitoreo en tiempo real:** proporciona dashboards interactivos y gráficos que permiten monitorear eventos de seguridad en tiempo real, facilitando la supervisión de sistemas y dispositivos críticos.

Vulnerability Manager Plus - Evaluación y gestión de vulnerabilidades

- **Evaluación de vulnerabilidades:** identifica y evalúa riesgos reales en la red, permitiendo una gestión proactiva de las amenazas.

- **Administración de parches:** facilita la descarga, prueba e implementación de parches en múltiples sistemas operativos y aplicaciones de terceros, asegurando que los sistemas estén actualizados y protegidos.

- **Gestión de la configuración de seguridad:** permite realizar un seguimiento de las alteraciones de configuración e implementar configuraciones seguras para eliminar brechas de seguridad.

Endpoint Central (versión Security) - Gestión integral de endpoints

- **Gestión unificada de endpoints:** automatiza rutinas regulares en la gestión de endpoints, incluyendo la instalación de parches, implementación de software y gestión de activos y licencias.

- **Seguridad de endpoints:** ofrece funciones de seguridad como protección ante ransomware, prevención de pérdida de datos y gestión de vulnerabilidades, fortaleciendo la postura de seguridad de la organización.

- **Control remoto y soporte:** permite el control remoto de máquinas y soporte simultáneo, mejorando la eficiencia operativa y la capacidad de respuesta ante incidentes.

Artículo 8: deberes específicos de los Operadores de Importancia Vital (OIV)

Este artículo establece una serie de obligaciones particulares para los llamados Operadores de Importancia Vital (OIV). Estas son entidades tanto públicas como privadas que gestionan infraestructuras esenciales para el funcionamiento del país, como servicios financieros, telecomunicaciones, energía, transporte, salud, entre otros.

Debido a su criticidad, estas instituciones deben adoptar medidas más rigurosas de seguridad para garantizar la continuidad operativa y proteger los datos e infraestructuras frente a ciberataques.

¿Cuáles son los principales deberes exigidos por este artículo?

1.Implementar un Sistema de Gestión de Seguridad de la Información (SGSI)

2.Planes de continuidad operacional y de ciberseguridad

3.Monitoreo y detección continua de amenazas

4.Medidas de mitigación ante incidentes

5.Capacitación continua y cultura de ciberseguridad

6.Notificación a las personas afectadas

7.Designación de un delegado de ciberseguridad

8.Certificaciones obligatorias

¿Cómo puede ayudar ManageEngine?

Log360 (SIEM)	• Proporciona **monitoreo en tiempo real** de eventos de seguridad en redes, servidores y endpoints, detectando actividades sospechosas o maliciosas. • Facilita la respuesta rápida a incidentes con análisis de logs centralizado, **alertas configurables** y correlación de eventos. • Automatiza la **generación de informes de cumplimiento**, fundamentales para auditar y mantener evidencia de acciones del SGSI.
Vulnerability Manager Plus	• **Permite priorizar y remediar riesgos**, alineándose con los requerimientos de un SGSI activo y enfocado en la prevención. • Incluye funciones de **gestión de parches**, verificación de configuración segura y seguimiento del ciclo de remediación.
Endpoint Central (versión Security)	• **Automatiza la aplicación de parches** críticos, el control de aplicaciones y el cifrado de discos, reduciendo el impacto y propagación de incidentes. • Permite ejecutar scripts para respuestas rápidas, bloqueos remotos y aislamiento de equipos comprometidos.
AD360	• **Gestiona eficientemente los accesos, roles y permisos** de usuarios a través del Directorio Activo, reduciendo las brechas de seguridad por errores humanos o privilegios innecesarios. • Proporciona **auditorías detalladas** de todas las acciones realizadas por los usuarios, lo cual es clave para demostrar el control interno del SGSI. • Refuerza la **protección de identidad**, uno de los pilares fundamentales para limitar accesos indebidos durante un incidente.

Artículo 9: deber de reportar incidentes de ciberseguridad

Establece uno de los pilares fundamentales de la Ley Marco de Ciberseguridad: la obligación de reportar incidentes de ciberseguridad con efecto significativo al CSIRT Nacional. Esta medida busca fortalecer la coordinación temprana, la transparencia y la capacidad de respuesta ante amenazas digitales, evitando que un ciberataque se propague o cause daños mayores.

¿Qué debe reportarse?

Se deben reportar todos los incidentes de ciberseguridad con efecto significativo, según lo definido en el Artículo 27 de la ley. Esto incluye, por ejemplo:

- Accesos no autorizados.
- Filtración o destrucción de datos.
- Ataques que afecten la continuidad del servicio.
- Uso indebido de privilegios.
- Compromisos de sistemas críticos.

Esquema de plazos para reportar un incidente

La Ley establece plazos estrictos y progresivos para comunicar un incidente al CSIRT Nacional:

a) Alerta temprana – dentro de 3 horas

Desde que la organización toma conocimiento del incidente, debe enviar una alerta inicial que informe sobre la existencia del evento. Este aviso no requiere todos los detalles, pero sí debe permitir al CSIRT activar mecanismos de coordinación si es necesario.

b) Informe preliminar – dentro de 72 horas

Se debe enviar una evaluación inicial con:

- Gravedad del incidente.
- Alcance o impacto estimado.
- Indicadores de compromiso (IoCs) identificados.

Los OIV (Operadores de Importancia Vital) cuyo servicio esencial se vea afectado deben enviar este informe preliminar en máximo 24 horas.

c) Informe final – dentro de 15 días

Incluye:

- Descripción completa del incidente.
- Evaluación de la gravedad.
- Causa probable o tipo de amenaza.
- Medidas de mitigación adoptadas o en ejecución.
- Repercusiones transfronterizas, si existen.

d) Incidentes en curso

Si el incidente aún no se ha resuelto al cumplir los 15 días, se entrega un informe de estado, y el informe final definitivo se presenta hasta 15 días después de haber sido gestionado el incidente.

e) Plan de acción (OIV) – dentro de 7 días

Los Operadores de Importancia Vital deben enviar el plan de acción adoptado para contener y remediar el incidente, dentro de los siete días siguientes a la detección.

¿Cómo puede ayudar ManageEngine?

Log360	• Genera alertas automáticas ante eventos críticos, cumpliendo con la exigencia de reportar en menos de 3 horas. • Almacena y organiza logs para facilitar la investigación forense y recopilación de IoCs (Indicadores de Copromiso), cuentas afectadas, IPs y detalles técnicos necesarios para los informes de 72 horas y 15 días. • Proporciona paneles de auditoría y generación de reportes automatizados.
OpManager **Site24x7** **Monitoreo de infraestructura**	• Detectan caídas, anomalías o cambios críticos en el rendimiento de redes, servidores, aplicaciones y servicios esenciales. • Complementan la alerta temprana permitiendo correlacionar problemas físicos con ciberincidentes. • Site24x7 aporta visibilidad desde la nube, ideal para infraestructuras híbridas.
ServiceDesk Plus Gestión de incidentes	• Permite gestionar todo el ciclo de vida del incidente con tickets, asignación de tareas, SLA y workflow. • Ayuda a cumplir con los plazos exigidos al documentar cada paso del proceso de respuesta en una línea de tiempo clara. • Facilita la colaboración entre equipos, la trazabilidad y la generación de informes para el CSIRT. • Incluye funciones de automatización para escalar alertas y asegurar el cumplimiento interno de tiempos.

Artículo 11: atribuciones de la ANCI

En este artículo se definen las facultades de la Agencia Nacional de Ciberseguridad (ANCI) para prevenir y gestionar incidentes. En particular, el literal *j)* establece una atribución crítica:

La ANCI podrá requerir a organismos públicos y a las instituciones privadas señaladas en el artículo 4 acceso a la información estrictamente necesaria para prevenir incidentes de ciberseguridad o gestionar uno que ya haya ocurrido.

Esto incluye la posibilidad de exigir el registro de actividades de redes y sistemas informáticos, con el fin de comprender en detalle qué ocurrió durante un incidente.

¿Qué implica esta atribución?

La ANCI tiene la potestad de fiscalizar técnicamente a las instituciones bajo su alcance, solicitando datos clave que permitan:

- Investigar causas de incidentes ocurridos.
- Identificar brechas o malas prácticas.
- Tomar medidas preventivas o correctivas.
- Coordinar acciones de respuesta.
- Asegurar la trazabilidad y la rendición de cuentas.

¿Cómo puede ayudar ManageEngine?

Log360 – Gestión centralizada de logs y SIEM	• Permite **recopilar, centralizar y conservar registros de eventos** y actividades generados por servidores, bases de datos, controladores de dominio, aplicaciones, dispositivos de red, entre otros. • Ayuda a cumplir con el requerimiento de la ANCI al generar **evidencia forense** estructurada, lo cual es clave para comprender incidentes. • Incorpora capacidades de **detección de amenazas**, correlación de eventos y **análisis de comportamiento de usuarios (UEBA)**, que permiten prevenir y gestionar ataques de forma proactiva. • Garantiza la integridad y seguridad de los logs, protegiéndolos contra alteraciones no autorizadas.
Network Configuration Manager (NCM) – Gestión y auditoría de configuraciones de red	• Permite **respaldar, versionar y auditar configuraciones** de routers, switches, firewalls y otros dispositivos de red críticos. • **Detecta cambios no autorizados** o sin aprobación, y mantiene un registro detallado de quién, cuándo y cómo se realizaron esos cambios. • Facilita el cumplimiento del artículo al proveer información precisa sobre el estado y la trazabilidad de la infraestructura durante o antes de un incidente. • Proporciona herramientas de automatización para **restaurar configuraciones** seguras rápidamente, reduciendo el impacto de un evento.

Firewall Analyzer – Visibilidad total sobre políticas y actividad de firewalls	• Proporciona **informes completos de tráfico**, reglas aplicadas, accesos permitidos/denegados y eventos sospechosos. • **Identifica reglas** obsoletas, redundantes o vulnerables que pueden generar brechas de seguridad. Contribuye a la gestión y documentación que puede ser requerida por la ANCI para verificar el **cumplimiento de estándares** y buenas prácticas. • Permite correlacionar la actividad en firewalls con logs y configuraciones, apoyando una investigación integral.

Artículo 27: incidentes de efecto significativo

El artículo 27 define con precisión cuándo un incidente de ciberseguridad se considera de efecto significativo, lo cual tiene implicaciones para su prioridad de respuesta y obligatoriedad de reporte.

¿Qué se considera un incidente de efecto significativo?

Según la Ley, un incidente será clasificado como significativo cuando:

- **Interrumpe la continuidad de un servicio esencial**, es decir, un servicio cuya interrupción puede generar consecuencias sociales, económicas o de seguridad relevantes.

- **Afecta la integridad física o salud de las personas**, lo que incluye, por ejemplo, ataques a sistemas hospitalarios o infraestructuras críticas.

- **Compromete sistemas informáticos que contengan datos personales**, con riesgo de exposición, pérdida o alteración de dicha información.

Este artículo activa múltiples responsabilidades legales para la organización afectada, como reportar al CSIRT Nacional (artículo 9), iniciar acciones de mitigación (artículo 8) y entregar información a la Agencia (artículo 11).

¿Cómo puede ayudar ManageEngine?

Log360 – Detección avanzada de amenazas y análisis de logs	• **Correlaciona eventos** en tiempo real para identificar comportamientos anómalos que podrían indicar un ciberataque, como accesos inusuales, cambios no autorizados o patrones de trÄfico sospechosos. • Genera **alertas personalizables** que ayudan a los equipos de seguridad a actuar antes de que un incidente escale a nivel significativo. • Permite identificar usuarios, dispositivos y sistemas involucrados, entregando trazabilidad completa para reportes y análisis. • Detecta accesos no autorizados a datos sensibles, como información personal, cumpliendo así con uno de los focos del artículo.
OpManager Plus – Monitoreo unificado de red, servidores y aplicaciones	• **Supervisa el estado de la infraestructura** crítica (como routers, servidores, bases de datos y servicios en la nube), permitiendo detectar fallas o degradaciones que puedan comprometer servicios esenciales. • Emite **alertas tempranas** en tiempo real cuando detecta interrupciones en el servicio, altos consumos de recursos o fallos de hardware/software que afecten la continuidad operativa. • Proporciona **dashboards visuales** para evaluar rápidamente el impacto potencial de una falla, ayudando a determinar si el incidente entra en la categoría de significativo.

Site24x7 – Observabilidad de aplicaciones, nube e infraestructura desde cualquier lugar	• Ofrece monitoreo desde una perspectiva externa, ideal para detectar caídas o lentitud en **servicios web**, APIs, sistemas en la nube o aplicaciones críticas accesibles por usuarios. • Evalúa en tiempo real la **disponibilidad de servicios esenciales** y la experiencia del usuario final, lo que permite correlacionar caídas con afectaciones potenciales al público o a servicios estratégicos. • Es especialmente útil para organizaciones con entornos híbridos o distribuidos, asegurando que los incidentes en **plataformas remotas** también sean detectados y reportados oportunamente.

Artículo 28: centros de certificación

El artículo 28 establece el marco institucional para asegurar que los Operadores de Importancia Vital (OIV) cumplan efectivamente con sus obligaciones de ciberseguridad a través de certificaciones emitidas por entidades acreditadas.

Este artículo indica qué:

- Los OIV deben obtener certificaciones de ciberseguridad obligatorias, conforme a lo que determine la ley y la Agencia Nacional de Ciberseguridad (ANCI) mediante reglamento.
- Estas certificaciones solo podrán ser emitidas por entidades certificadoras autorizadas, registradas oficialmente por la ANCI.
- La Agencia acreditará estas entidades certificadoras, estableciendo requisitos que deberán mantener en el tiempo.
- Adicionalmente, la Agencia podrá reconocer u homologar certificaciones internacionales, permitiendo que estándares globales como ISO 27001, NIST, o similares puedan ser utilizados como referencia válida para cumplimiento local.

Este artículo busca que los OIV validen técnicamente, mediante terceros autorizados, que sus planes de ciberseguridad, continuidad operativa y SGSI estén implementados de acuerdo con estándares reconocidos y auditables.

¿Cómo puede ayudar ManageEngine?

Aquí es donde las soluciones de ManageEngine resultan fundamentales: permiten implementar, monitorear y cumplir con controles clave exigidos en estándares como ISO/IEC 27001, PCI-DSS, HIPAA, GDPR, NIST, entre otros, lo que facilita los procesos de auditoría y certificación.

Ecosistema de soluciones de ManageEngine

Soluciones de cumplimiento

ManageEngine ofrece funcionalidades específicas para facilitar el cumplimiento con regulaciones y estándares internacionales. Entre ellas:

- Auditoría de cambios y accesos (Log360, AD360)
- Gestión de vulnerabilidades (Vulnerability Manager Plus)
- Seguridad en endpoints (Endpoint Central)
- Gestión de identidades y accesos (AD360)
- Controles de red y configuración (OpManager, Network Configuration Manager)
- Documentación y trazabilidad de procesos (ServiceDesk Plus)

Estas herramientas ayudan a cubrir múltiples controles requeridos en procesos de certificación como los de ISO 27001 (control de accesos, gestión de activos, continuidad del negocio, control de cambios, gestión de incidentes, etc.).

Artículo 32: deber de reporte al CSIRT de la Defensa Nacional

Este artículo establece un régimen específico de notificación de incidentes para las instituciones de la Defensa Nacional, similar al contemplado en el artículo 9 para el resto del ecosistema.

Señala que:

- Las instituciones del ámbito de la Defensa Nacional (Ejército, Armada, Fuerza Aérea y otras dependencias) deberán reportar ciberataques o incidentes de ciberseguridad significativos al CSIRT de la Defensa Nacional.

- A su vez, este CSIRT sectorial deberá informar a la Agencia Nacional de Ciberseguridad (ANCI) sobre aquellos incidentes que no comprometan la seguridad o defensa nacional, según lo que establezca el reglamento.

Este modelo busca mantener la coordinación nacional en materia de ciberseguridad, respetando las restricciones propias del ámbito militar, como el manejo de información clasificada o crítica para la seguridad del país. En la práctica, se establece una cadena de escalamiento interno, donde el CSIRT de Defensa actúa como filtro y enlace ante la Agencia.

¿Cómo puede ayudar ManageEngine?

Aunque el entorno militar tiene requisitos particulares de seguridad y confidencialidad, las capacidades tecnológicas necesarias para cumplir con este deber de reporte son equivalentes a las que se requieren en el sector civil: detección temprana, trazabilidad, análisis forense y gestión coordinada de incidentes.

Las siguientes herramientas de ManageEngine ofrecen funcionalidades críticas que pueden ser utilizadas por las instituciones de defensa para facilitar el cumplimiento de este artículo:

Log360	• Monitorear en tiempo real las actividades sospechosas dentro de redes y sistemas clasificados o estratégicos. • Generar alertas inmediatas ante intrusiones o comportamientos anómalos. • Centralizar y conservar logs para una respuesta rápida y trazable ante incidentes, generando información clave para los informes que se deben elevar al CSIRT Defensa.
OpManager / Site24x7	**Soluciones de monitoreo proactivo de infraestructura y servicios críticos. Pueden ser empleadas para:** • Vigilar la disponibilidad y funcionamiento de sistemas de mando, comunicaciones o plataformas críticas de defensa. • Detectar anomalías de rendimiento o caídas inusuales que puedan estar relacionadas con ciberataques. • Complementar la alerta temprana ante incidentes que afectan la continuidad de operaciones estratégicas.
ServiceDesk Plus	**Sistema de gestión de incidentes TI con flujos de trabajo estructurados. Puede ser usado para:** • Registrar y documentar cada evento de ciberseguridad de forma trazable. • Asignar tareas automáticamente a los equipos de respuesta del CSIRT Defensa. • Mantener una bitácora detallada de cada fase del proceso de reporte (detección, análisis, mitigación, comunicación).

Artículo 33: la reserva de información

El artículo 33 establece la confidencialidad legal de toda la información sensible relacionada con ciberseguridad que esté en poder de:

- La Agencia Nacional de Ciberseguridad (ANCI).
- El CSIRT Nacional.
- El CSIRT de la Defensa Nacional.
- Y otros organismos de la Administración del Estado.

Este deber de confidencialidad alcanza tanto a los documentos como a los datos y registros, y también se extiende al personal que accede a dicha información en el ejercicio de sus funciones.

Además, declara expresamente como información clasificada y de circulación restringida los siguientes elementos críticos:

i) Las matrices de riesgos de ciberseguridad.

ii) Los planes de continuidad operacional y planes de respuesta a desastres.

iii) Los planes de acción y mitigación de riesgos de ciberseguridad.

Este artículo protege legalmente la confidencialidad de la información estratégica que sustenta la defensa cibernética del Estado chileno. Su filtración podría representar una amenaza para la seguridad pública o nacional.

¿Cómo puede ayudar ManageEngine?

Log360 (módulo DLP y clasifi-cación de datos sensibles)	Permite identificar archivos y registros que contengan información crítica, como matrices de riesgo o planes de continuidad. Aplica políticas de clasificación, monitoreo y protección para evitar el acceso o uso no autorizado. Cuenta con capacidades de auditoría forense y alertas en tiempo real ante actividades sospechosas.
DataSecurity Plus	Monitorea de forma continua el acceso a archivos confidenciales en servidores y carpetas compartidas. Detecta y reporta intentos de lectura, modificación, copia o borrado de documentos clasificados. Permite generar alertas ante accesos fuera de horario, desde ubicaciones no autorizadas o por usuarios no validados.
Endpoint Central (controles de CIS y DLP)	Aplica controles preventivos en estaciones de trabajo y laptops para evitar filtraciones accidentales o intencionales. Permite restringir el uso de dispositivos USB, aplicaciones, navegación web y el movimiento de archivos críticos. Se alinea con controles de CIS Benchmarks, ayudando a asegurar los endpoints donde se almacena o manipula información reservada.

Artículo 34: extensión de la obligación de reserva

Este artículo amplía la obligación de confidencialidad establecida en el artículo 33. Específicamente, señala que:

"La obligación de guardar secreto se extiende también a aquellas personas que, sin ser parte de la Agencia ni de los CSIRT, tengan conocimiento de solicitudes o medidas especiales para la obtención de información de ciberseguridad."

Esto incluye, por ejemplo:

- Personas externas que acceden a información en el marco de un proceso judicial o fiscalización.
- Proveedores o auditores externos que, por razones legales o contractuales toman conocimiento de datos clasificados o acciones reservadas.
- Funcionarios de otras entidades que colaboren temporalmente con la Agencia o CSIRTs.

El objetivo de este artículo es proteger la confidencialidad incluso cuando la información reservada transite fuera de los organismos estatales principales. Cualquier persona que acceda a estos datos por razones legales queda obligada a guardar secreto bajo las mismas condiciones que los funcionarios públicos.

¿Cómo puede ayudar ManageEngine?

PAM360 – Privileged Access Management (gestión de acceso privilegiado)

Funcionalidades clave para cumplir el Art. 34:

- **Control y monitoreo de accesos privilegiados** a recursos críticos como servidores, bases de datos, switches, firewalls y consolas administrativas.
- Acceso "just-in-time": entrega credenciales temporales para terceros autorizados, que caducan automáticamente.
- **Sesiones grabadas:** registra todo lo que hace un usuario con acceso privilegiado, permitiendo auditoría completa posterior.
- **Seguridad de credenciales:** gestiona de forma centralizada las contraseñas sensibles, evitando su exposición innecesaria.
- **Control de aprobaciones:** el acceso de terceros puede requerir la autorización previa de un supervisor designado.

Un Digital Workplace para enfrentar los desafíos de ciberseguridad

Si bien nombramos diversas herramientas que pueden ayudarte a cumplir con distintos aspectos de esta Ley, uno de los grandes desafíos para muchas organizaciones es la falta de integración entre ellas.

La gestión fragmentada de soluciones puede generar silos de información, duplicidad de esfuerzos, menor eficiencia operativa y una respuesta más lenta ante incidentes.

Aquí es donde el **Digital Workplace de ManageEngine** marca una diferencia significativa.

Se trata de un entorno de trabajo digital completamente integrado que combina en un solo ecosistema todas las herramientas necesarias para la gestión de identidades, monitoreo de infraestructura, seguridad de endpoints, cumplimiento normativo, gestión de vulnerabilidades, automatización del soporte técnico y mucho más.

Esta sinergia tecnológica te permitirá cumplir con las exigencias de la ley de forma más ágil y centralizada.

Con el Digital Workplace de ManageEngine podrás:

- Tener una visión holística de la ciberseguridad y la infraestructura de TI.
- Reducir tiempos de respuesta ante incidentes al contar con flujos de trabajo unificados.
- Simplificar auditorías y reportes exigidos por la normativa.
- Aumentar la eficiencia operativa al evitar soluciones desconectadas y procesos manuales.
- Mantener un entorno alineado con estándares internacionales, facilitando el camino hacia certificaciones reconocidas.

En lugar de implementar soluciones aisladas, puedes optar por una plataforma robusta, modular y escalable, diseñada para los desafíos actuales de ciberseguridad y cumplimiento.

Descubre aquí más sobre cómo el Digital Workplace de ManageEngine puede ayudarte a construir una operación de TI más segura y colaborativa.

Conclusión

La Ley Marco de Ciberseguridad marca un antes y un después en la manera en que Chile enfrenta los desafíos del entorno digital. Su promulgación no solo responde a la creciente necesidad de proteger la infraestructura crítica y los datos sensibles, sino que establece un marco claro de responsabilidades, coordinación y acción para todos los actores del ecosistema nacional.

Comprender esta ley y prepararse para su cumplimiento no es solo una obligación legal, sino una oportunidad estratégica para fortalecer la resiliencia organizacional, generar confianza y adoptar una cultura de seguridad alineada con los estándares internacionales.

En un mundo donde las amenazas cibernéticas evolucionan constantemente, estar preparados ya no es una ventaja, sino una condición esencial para operar con responsabilidad y una visión hacia el futuro.

Este contenido fue realizado por:

Paola Andrea Quiroga
Marketing Analyst
ManageEngine LATAM

Acerca de ManageEngine

ManageEngine desarrolla el conjunto de software de gestión de TI más completo de la industria. Tenemos todo lo que necesita: más de 90 productos y herramientas gratuitas para gestionar todas sus operaciones de TI, desde redes y servidores hasta aplicaciones, mesa de ayuda, Active Directory, seguridad para desktops y dispositivos móviles.

Desde 2001, los equipos de TI como el suyo han recurrido a nosotros para obtener un software asequible, rico en funciones y fácil de usar. Puede encontrar nuestras soluciones on-premises y en la nube que impulsan la TI de más de 180.000 empresas en todo el mundo, incluidas nueve de cada diez empresas de la lista Fortune 100.

A medida que usted se prepara para los desafíos de la gestión de TI que se avecinan, nosotros lideraremos el camino con nuevas soluciones, integraciones contextuales y otros avances que solo pueden provenir de una empresa dedicada singularmente a sus clientes. Y al ser una división de Zoho Corporation, seguiremos trabajando por establecer una estrecha alineación de TI con los negocios que usted necesitará para aprovechar las oportunidades en el futuro.

ManageEngine

www.manageengine.com/latam/