ARTION
Aplicando la Experiencia

¿Cómo cumple una empresa la ley Marco de Ciberseguridad 21.663?

Los 4 pilares que toda organización debe implementar según la nueva normativa chilena

Gobernanza y Roles
Lo que la organización debe tener

Gobierno de Ciberseguridad Formal
- *Políticas*
- *Roles*
- *Responsabilidades*

Responsable de Ciberseguridad Designado
- *Interno o*
- *Externo*

Politicas Obligatorias
- *Gestión de Riesgos*
- *Continuidad Operativa*
- *Seguridad de la Información*
- *Gestión de Incidentes*

Registro de Activos Críticos
- *Políticas*
- *Roles*
- *Responsabilidades*

Controles Mínimos de Ciberseguridad
Lo que la organización debe implementar

Prevención
- Gestión de identidades y accesos (MFA obligatorio).
- Hardening de equipos y servidores.
- Segmentación de redes.
- Control de cambios.
- Cifrado de datos sensibles.

Detección
- Monitoreo continuo de eventos relevantes.
- Registros (logs) centralizados.
- Herramientas de detección de amenazas (SIEM/SOC u otro mecanismo equivalente).

Respuesta
- ·Plan formal de respuesta a incidentes.
- ·Equipo responsable y procedimientos (playbooks).
- ·Capacidad de contener, erradicar y recuperar.

Operación
- ·Backups probados periódicamente.
- ·Plan de Continuidad Operativa (BCP).
- ·Plan de Recuperación ante Desastres (DRP).
- RTO/RPO definidos.

Reportabilidad y Obligaciones ante ANCI
Lo que la organización debe hacer

- Notificar incidentes relevantes a la Agencia Nacional de Ciberseguridad (ANCI) en los plazos establecidos.
- Mantener capacidad de trazabilidad de incidentes.
- Reportar brechas de seguridad que afecten servicios esenciales.
- Participar en auditorías, fiscalizaciones y requerimientos de la ANCI.

Cultura y Formación
El Motor del Cumplimiento

- Programas de capacitación obligatoria para todo el personal.
- Concientización continua (phishing, buenas prácticas, uso seguro de sistemas).
- Inclusión de Ciberseguridad en la inducción de nuevos colaboradores.
- Simulacros y pruebas de madurez operativa.

Cumplir con la Ley Marco de Ciberseguridad 21.663 no es solo un requisito legal: es una inversión en continuidad, reputación y resiliencia operativa.