Desafíos técnicos de la implementación en las empresas de los requerimientos de la Ley Marco de Ciberseguridad

Alfonso Mateluna[i]

Si su empresa o institución, sea pública o privada, está dentro del alcance de la infraestructura critica, está afecta a la Ley Marco de Ciberseguridad, la cual, entre otros, establece:

1. Creación de la Agencia Nacional de Ciberseguridad (ANCI)

- Función: Coordinar y supervisar la implementación de la política de ciberseguridad en Chile[1].
- Responsabilidades: Regular, fiscalizar y sancionar a los organismos públicos y privados que presten servicios esenciales[1].

2. Sistemas de Gestión de Seguridad de la Información

- Requisitos: Las entidades deben implementar sistemas de gestión de seguridad de la información, realizar evaluaciones de riesgo continuas y desarrollar planes de respuesta a incidentes[2].

3. Reportes Obligatorios de Incidentes

- Obligación: Las entidades deben reportar incidentes de ciberseguridad a la ANCI de manera oportuna[2].

4. Medidas Preventivas y de Contención

- Implementación: Las organizaciones deben adoptar medidas preventivas para proteger sus activos informáticos y contener posibles incidentes[3].

5. Capacitación y Concientización

- Requisito: Las empresas deben capacitar a su personal en prácticas de ciberseguridad y concientización sobre los riesgos cibernéticos[3].

6. Principios Rectores

- Incluyen: Seguridad en el ciberespacio, respuesta responsable y coordinada ante incidentes, y seguridad y privacidad por defecto y desde el diseño[4].

7. Diferenciación para PYMEs

- Medidas Adaptadas: La ANCI establecerá medidas de seguridad diferenciadas según el tipo de organización, considerando las características y capacidades de las pequeñas y medianas empresas (PYMEs)

Lo anterior implica tomar medidas con las cuales dimensionar, costear y prepararse para el cumplimiento:

A. ¿Tiene identificados sus procesos, sistemas, infraestructura y activos críticos?, si es así, ¿están adecuadamente protegidos y respaldados según su nivel de criticidad?
B. Seguramente deberá hacer una revisión de estado inicial de seguridad y continuidad de procesos; con ello, establecer un plan priorizado de nivelación de seguridad y continuidad; buscar presupuesto entendiendo que no es un desafío para la gerencia de sistemas, sino que para toda la institución.
C. Validar que los niveles de protección mínima estén aplicados en las instalaciones de TI como de OT; generalmente hay un desnivel en la aplicación de medidas de protección, resiliencia y recuperación entre tales ambientes.
D. Identificar la infraestructura con obsolescencia; es un tema que afecta transversalmente a las organizaciones y que tiene doble implicancia; no posee parches ni actualizaciones por el fabricante (existen parches virtuales y otras soluciones), y fallas de partes y componentes, ambas causantes de interrupción de servicios y contingencias difíciles de resolver: defina medidas paliativas de corto plazo; así como de mediano y largo plazo, acordes al plan estratégico de su organización.
E. Deberá fortalecer su capacidad de monitoreo de procesos, anticipándose a incidentes y diagnosticando y solucionando causas raíces de fallas en sus procesos.
F. Deberá adoptar un Sistema de Gestión de Seguridad de la Información, apoyándose en la última versión de la ISO 27001; con un alcance que cubra las actividades de cara a su giro que lo califica como infraestructura crítica.
G. Conozca qué se dice de usted en Deep Web y foros de Telegram; podrá anticiparse a ataques de hacktivismo; qué se dice de las fallas que han encontrado en su seguridad perimetral e interna.
H. Concientice a su personal en materias de seguridad, ciberseguridad, recuperación, identificación y escalamiento de incidentes de seguridad y ciberseguridad; capacite a su personal que está a cargo de sus sistemas e infraestructura crítica.
I. Parchado de su infraestructura, renovación tecnológica y cifrado de la información sensible serán sus grandes aliados.
J. Establezca un ecosistema de proveedores críticos que posean certificaciones en seguridad; valide que mantengan vigentes sus certificaciones y auditorías de terceros sobre cumplimiento con marcos y estándares de seguridad y resiliencia.
K. Identifique y fortalezca sus puntos únicos de falla; aquellos que si fallan o son atacados puedan poner en jaque su seguridad y continuidad.
L. Revise y escanee periódicamente sus servicios de cara a internet; así como sus sistemas internos e infraestructura soportante; establezca planes de mitigación con fechas claras y proporcionales a la criticidad de los hallazgos; de visibilidad de dicho plan y su seguimiento al directorio de la institución.
M. Redefina sus metodologías de ciclo de vida y desarrollo de sistemas, para incluir el principio de seguridad y privacidad por defecto y por diseño; revise en sus sistemas que ya existen cuáles son las potenciales brechas en términos de privacidad y seguridad.

Ser infraestructura crítica implica un valor estratégico a preservar para el normal funcionamiento del país, su economía, servicios básicos y bienestar de la población.

---

[i] Ingeniero. Profesor del Diplomado de Regulación y Tecnología UDD. Director de ISACA Santiago Chile.