Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (Boletín N°14.847-06)

Claudio Magliona

ACTI
Asociación Chilena de Empresas de Tecnologías de Información A.G.

CONSIDERACIONES GENERALES

La Asociación Chilena de Empresas de Tecnología de Información A.G. es la principal comunidad de empresas de la industria de tecnologías de la información y telecomunicaciones del país, formando parte de diversos rubros como el hardware, el software, la capacitación e integración de sistemas e internet.

Como gremio, apoyamos la necesidad de crear un marco regulatorio robusto que aborde la ciberseguridad en nuestro país, pero como toda iniciativa legal creemos debe perfeccionarse para dar certeza jurídica a los regulados en el ecosistema digital y en ese sentido consideramos positivo revisar algunas preocupaciones.

PREOCUPACIONES:

1) Muy Extenso Ámbito de Aplicación de la Ley General:

- Art. 1°: ámbito de aplicación.
- No encontramos antecedente similar en derecho comparado: NIS 1 Y NIS 2 establecen alcance a entidades u operadores de carácter esencial/importante, aplicando distintas reglas.
- Creemos que una pyme, almacén, panadería no debería tener obligación de comunicar vulnerabilidades ni en 3 horas ni en el tiempo que finalmente se decida.
- No comunicar incidentes se sanciona como infracción grave, desde 1.001 UTM (artículo 33)
- Entendemos que la agencia puede eximir de estas obligaciones o dar tratamiento a ciertas entidades, pero esta es una ley que de **debe aplicar a servicios esencial y operadores vitales**. Queremos evitar discrecionalidades y tener certezas jurídicas.

PREOCUPACIONES

2) Importancia Igualdad ante la ley. Exclusión de aplicación a empresas públicas, estatales o con participación:

- ¿Por qué una institución privada que no sea operadora de importancia vital está obligada a reportar y una empresa pública que no es calificada operadora de importancia vital no debe reportar?
- Tratamiento especial genera confusión, pues:
  - Art. 33° sobre infracciones, letra c) infracciones gravísimas no distingue sanción para infractor operador de importancia vital (infracciones leves y graves sí), ¿eso quiere decir que no se sanciona?
  - Art. 34° Proc. Administrativo por infracción a la ley que cometan instituciones privadas: ¿significa que empresas públicas calificadas como operadores importancia vital no se aplica este procedimiento?

3) Se requiere revisión general del proyecto. Proyecto contempla definiciones en catálogo que no se aplican nuevamente en todo el cuerpo: Activo informático, No repudio, Interagencialidad. Además artículo 21 literal j utiliza término "acarreará responsabilidad". Artículo 1 inciso 3 "seguridad informática de las personas y sus familias".

4) Proceso de determinación de Servicios Esenciales:

- ¿Por qué no detallarlos? ¿Qué pasa con seguridad Jurídica?
- No sigue estándar internacional que tiene detalle en Anexos:

- Directiva (UE) 2016/1148: Ver Anexo II en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32016L1148#d1e32-27-1
- NIS 2: Ver Anexo I en: https://eur-lex.europa.eu/eli/dir/2022/2555#d1e32-143-1
- + Sin catálogo previamente definido, ¿por qué no contemplar un mecanismo de impugnación especial para entidades calificadas como importante o esencial? (como sí contempla normativa Española 8/2011 por ejemplo?.

PREOCUPACIONES

5) Deber de reportar en plazo inferior a 3 horas (artículo 7):

- No existe antecedente en derecho comparado de plazo tan breve. Además se debería distinguir en criticidad del incidente para fijar tiempo. Hay incidentes que no pasan de ser un incidente sin afectación, otros son incidentes habilitantes parciales y otros totales.
- NIS 2, art. 20° es gradual: *a) notificación "sin dilación indebida"; b) una notificación temprana (plazo de 24 hrs), y luego una notificación del incidente dentro de 72 horas que actualice la información entregada en la advertencia temprana y que indique: un análisis inicial del incidente; su severidad e impacto; y cuando sea posible los indicadores de compromiso; c) un reporte intermedio a petición del CSIRT o autoridad competente; y d) un reporte final (plazo de un mes).*

6) Art. 3° n° 11 Principio del Cifrado: *toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado. Ninguna persona ni autoridad podrá afectar, restringir o impedir el ejercicio de este derecho.*

- Preocupa: ¿Qué significa que nadie pueda restringir el cifrado? ¿Qué relación tiene con este Proyecto? Investigación de un delito de pornografía infantil, efectos?

7) Certificaciones: ¿organismos autorizados para certificar súnicamente las acreditadas por la Agencia? (art. 24°)

- ¿homologación proceso? O ¿hay certificaciones de tal calidad que no requieren homologación?
- ¿Obligatorias para todos?: En NIS 2 Directive Art. 24, las certificaciones sean obligación únicamente señalada para entidades de importancia o esenciales.

PREOCUPACIONES

8) Infracciones y Sanciones (art. 33°):

- Propender a un catálogo preciso y definido de conductas infraccionales y sus respectivas sanciones, con catálogo de circunstancias atenuantes y agravantes.
- Consideramos positivo revisar catálogo siguiendo así recomendaciones de Corte Suprema: garantizar principios de tipicidad y proporcionalidad.
- Inclusive ver literal c) de artículo 33 en materia de infracciones gravísimas, donde no se habla de operadores de importancia vital.

9) Facultades de la Agencia (Art. 9° inciso segundo):

- *Artículo 9°. Atribuciones. Para dar cumplimiento a su objeto, la Agencia tendrá las siguientes atribuciones: (…)*

Inciso segundo: ***La Agencia contará con todas las facultades que fueren necesarias*** *para el cumplimiento de su función fiscalizadora, entre otras, (…)*

- Así de amplio podría diluir mandato de art. 2° de Ley de Bases Generales de la Adm. Del Estado: órganos de la Adm. Deberán actuar dentro de su competencia y no tendrán más atribuciones que las que expresamente les haya conferido ordenamiento jurídico.

PREOCUPACIONES

10) HACKING ÉTICO. Modificación ley 21.459:

- No estamos de acuerdo que se permita acceder a un sistema de tratamiento de la información eludiendo medidas de protección. Esto se discutió durante la discusión de la nueva ley de delitos informáticos.
- Respecto de la norma de Bélgica que el proyecto esta siguiendo, cabe hacer presente que solo permite que un hacking ético tenga lugar en empresas con domicilio y residencia en Bélgica. Porqué? Porque de lo contrario Bélgica podría convertirse en un puerto seguro de hackeo de empresa y organismos públicos de todo el planeta. Nuestro llamado es a revisar detalladamente los efectos que puede tener una norma de esta naturaleza en Chile.

11) Asimismo llama la atención la siguiente norma. Modificación ley 21.459:

- *"Tampoco será objeto de sanción penal la persona que comunique a la Agencia información sobre una vulnerabilidad potencial de la que haya tomado conocimiento en su contexto laboral o con ocasión de la prestación de sus servicios, ni se considerará que ha incumplido con ello su obligación de secreto profesional."."*
- **Entendemos el propósito, pero primero, tiene que informar a la entidad. Tiene que haber procedimiento interno, de lo contrario, esto se puede prestar para abusos. Esto es otra demostración del porque esta normativa solo debe aplicar a servicios esenciales y operadores vitales.**

PREOCUPACIONES

12) Período de Vacancia:

- Consideramos positivo contar con plazo que permita la debida adecuación a la normativa.
- Sobre todo, considerando que Chile va 20 años tarde en comparación a la normativa internacional sobre la materia.
- Por ello, sugerimos seguir estándares internacionales en que plazo de implementación y cumplimiento van entre los 21 a 32 meses. Ejemplos:

- la Directiva UE 2008/114/CE: de 8 de diciembre de 2008, contempló para cumplimiento hasta enero de 2011. (25 meses aprox.)
- la Directiva (UE) 2016/1148: de 6 de julio de 2016, contempló para cumplimiento hasta mayo de 2018. (22 meses aprox.)

- **¿preguntas?**

- **Saludos y muchas gracias y vamos por un Chile más seguro!**

¡Gracias!