OBSERVACIONES AL PROYECTO DE LEY QUE REGULA LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

Seminario: Hacia una regulación de la inteligencia artificial en Chile

Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación — Senado de la República

Paulina Assmann — CEO/Cofundadora, SeQure Quantum | 24 de abril de 2026

1. Contexto: una ley que define la infraestructura digital de las próximas décadas

El proyecto de ley aprobado por la Cámara de Diputados (Boletines N° 15.869-19 y 16.821-19) representa un avance significativo para Chile. Su enfoque basado en riesgos es correcto: protegerse y anticiparse es fundamental.

Sin embargo, esta ley no solo regula una tecnología. Define la infraestructura digital de los próximos 20 a 30 años. Y en ese horizonte, el marco normativo debe ser capaz de cumplir dos objetivos simultáneos que no son contradictorios: resguardar la seguridad de los datos y permitir que Chile sea parte del mayor ciclo de inversión tecnológica de la historia.

La inteligencia artificial es desarrollo, pero también confianza. Y para que esa confianza exista, el marco regulatorio debe evolucionar junto con la tecnología. Hoy vemos cómo distintas regiones, particularmente en Europa, están revisando sus marcos regulatorios porque un enfoque excesivo en el riesgo puede terminar ralentizando la innovación. Ese es un aprendizaje que Chile debe considerar.

> ***Esta ley debe ser, al mismo tiempo, una protección y una oportunidad. Una oportunidad para que empresas chilenas compitan en mercados globales con un marco regulatorio alineado con estándares internacionales.***

2. El punto ciego: la convergencia entre IA y computación cuántica

El proyecto clasifica adecuadamente los riesgos de los sistemas de IA convencionales. Sin embargo, tiene un punto ciego estructural: no contempla qué ocurre cuando la base de la seguridad digital —la criptografía— deja de ser confiable frente a sistemas de inteligencia artificial cada vez más capaces, y en particular, frente al momento en que la IA comience a utilizar capacidades de computación cuántica.

Chile es uno de los países más conectados de América Latina. Gran parte de nuestra actividad —financiera, productiva e institucional— depende de sistemas digitales que transmiten información permanentemente. Ese nivel de conectividad es una fortaleza, pero también implica una mayor exposición.

Existen tres riesgos concretos y presentes que el proyecto actual no contempla:

2.1 Harvest Now, Decrypt Later (HNDL): un riesgo presente, no futuro

En el contexto de la transmisión de datos —comunicaciones financieras, de salud, de infraestructura crítica— la información viaja cifrada a través de redes que hoy consideramos seguras. Sin embargo, actores maliciosos están capturando ese tráfico cifrado hoy, almacenándolo, con el objetivo de descifrarlo cuando existan capacidades suficientes. Los sistemas de IA están acelerando esta recolección y clasificación de datos a gran escala.

Esto significa que información sensible que se transmite hoy, aunque esté protegida, puede quedar expuesta en el futuro. La ley no menciona este vector en ninguna de sus categorías de riesgo.

Referencia: *NSA, "Quantum Computing and Post-Quantum Cryptography", 2022; ENISA, "Post-Quantum Cryptography: Current State and Quantum Mitigation", 2021.*

2.2 Cambio estructural en la capacidad de procesamiento

La evolución hacia sistemas donde la inteligencia artificial puede apoyarse en capacidades de computación cuántica no implica un salto inmediato, pero sí un cambio estructural en la capacidad de procesar información, identificar patrones y resolver problemas complejos. Ese cambio impacta directamente los supuestos sobre los que hoy se construye la seguridad digital, incluyendo los algoritmos criptográficos que protegen la infraestructura crítica nacional.

2.3 Vulnerabilidad de la infraestructura crítica

Sectores como energía, banca y telecomunicaciones operan sobre sistemas diseñados bajo supuestos de seguridad que dejarán de cumplirse. El artículo 16 del proyecto define como incidente grave la afectación de infraestructura crítica. Sin embargo, el artículo 9 no exige evaluación de resiliencia frente a este escenario. Chile estaría declarando crítica una infraestructura que sabemos deberá adaptarse en el corto y mediano plazo, sin exigir que esa adaptación forme parte del marco regulatorio.

Referencia: *NIST FIPS 203/204/205, 2024; McKinsey Global Institute, "The Quantum Technology Monitor", 2025.*

3. Contexto internacional: inversión y estándares en curso

Esta discusión no ocurre en un vacío. Estamos frente a una de las mayores olas de inversión tecnológica de la historia.

Inteligencia Artificial	Computación Cuántica
Más del 61% del capital de riesgo global en 2025	USD 2.000 millones en startups cuánticas en 2024 (+50% vs 2023)
USD 258.700 millones en inversión VC (OCDE, 2026)	USD 10.000 millones en compromisos públicos globales a abril 2025
Gasto global proyectado: USD 1,5 billón en 2025 (Gartner)	Mercado proyectado: USD 97.000 millones al 2035 (McKinsey)

Estos números muestran algo muy claro: la inteligencia artificial es el motor de desarrollo. Y Chile debe posicionarse para ser parte de ese desarrollo. Pero también muestran que la

computación cuántica ya es una industria en formación, con inversiones estatales de primer orden que no podemos ignorar.

A nivel normativo, Estados Unidos, a través del NIST, publicó en 2024 los primeros estándares de criptografía post-cuántica (FIPS 203, 204 y 205) y definió una hoja de ruta de migración hacia estos estándares para el año 2030. Europa avanza en la misma dirección a través del Cyber Resilience Act y NIS2.

Chile no incorpora esta transición ni en este proyecto de ley ni en la Ley Marco de Ciberseguridad. Si aprobamos este marco sin considerarla, nace desactualizado respecto de los estándares internacionales vigentes.

> ***Como empresa tecnológica nacida en Chile, hoy estamos trabajando para entrar al mercado de Estados Unidos. Y en ese proceso es evidente: los mercados más avanzados están exigiendo estándares claros en seguridad, particularmente en lo que respecta a la transición hacia tecnologías resistentes a la computación cuántica. Cuando Chile se alinea con esos estándares, no solo regula. Abre puertas.***

4. Propuesta: incorporar una categoría de Riesgo Cuántico

Se propone al Senado incorporar en el proyecto una quinta categoría de riesgo, denominada Riesgo Cuántico, sin rediseñar el marco existente sino actualizándolo. La definición propuesta es la siguiente:

> *"Riesgo cuántico: el uso de sistemas de IA que puedan invocar capacidades de computación cuántica como parte de su operación, o que operen en contextos donde la criptografía que protege la infraestructura subyacente sea vulnerable a dichas capacidades, en ámbitos de infraestructura crítica, datos sensibles o seguridad nacional."*

Esta categoría impondría tres obligaciones concretas:

1. **Migración a algoritmos de criptografía post-cuántica estandarizados:** los operadores de sistemas de alto riesgo que operen sobre infraestructura crítica o manejen datos sensibles deberán migrar hacia algoritmos PQC estandarizados por el NIST (FIPS 203, 204 y 205) o equivalentes reconocidos internacionalmente. Esta migración deberá ser progresiva, documentada y sujeta a revisión periódica, en línea con la hoja de ruta definida por EE.UU. para el año 2030.

2. **Evaluación de resiliencia post-cuántica:** como componente obligatorio del sistema de gestión de riesgos del artículo 9, que incluya una revisión de los algoritmos criptográficos utilizados y su vulnerabilidad frente a capacidades cuánticas actuales y proyectadas.

3. **Registro diferenciado ante la APDP y la ANCI:** para sistemas que puedan invocar capacidades cuánticas o que implementen criptografía post-cuántica, con

mecanismos de supervisión adecuados, reporte de incidentes específicos y verificación del avance en los planes de migración.

5. Referencias internacionales seleccionadas

Fuente	Año	Relevancia
NIST FIPS 203, 204, 205	2024	Primeros estándares PQC definitivos; hoja de ruta de migración al 2030
NSA — Quantum Computing and Post-Quantum Cryptography	2022	Marco de transición para infraestructura crítica frente a amenaza cuántica
ENISA — Post-Quantum Cryptography	2021	Evaluación europea de amenazas HNDL y hoja de ruta regulatoria
McKinsey — Quantum Technology Monitor	2025	Proyecciones de mercado cuántico: USD 97.000M al 2035
OCDE — Venture Capital Investments in AI through 2025	2026	IA capta el 61% del capital de riesgo global; USD 258.700M en 2025
Gartner — Worldwide AI Spending	2025	Gasto global en IA proyectado en USD 1,5 billón para 2025
EU Cyber Resilience Act + NIS2	2024	Incorporación de resiliencia post-cuántica en regulación europea

6. Conclusión

Chile tiene una oportunidad única: no solo ser el primer país de América Latina con una ley de inteligencia artificial, sino ser el primero en anticipar correctamente la siguiente etapa tecnológica.

Incorporar la categoría de Riesgo Cuántico, con una exigencia explícita de migración a algoritmos PQC estandarizados, no representa una carga adicional para la innovación. Es una señal de madurez regulatoria que alinea a Chile con los estándares internacionales vigentes y que, al mismo tiempo, abre puertas a los mercados más exigentes del mundo.

La inteligencia artificial es el motor del desarrollo que viene. Y Chile debe posicionarse para ser parte de él, con un marco regulatorio que proteja sin frenar, que anticipe sin sobrecargar, y que permita a las empresas chilenas competir con las mismas reglas que los mercados más avanzados ya están adoptando.

La pregunta no es si esta transición ocurrirá. La pregunta es si queremos prepararnos a tiempo, o adaptarnos cuando ya sea inevitable.

Paulina Assmann
CEO y Cofundadora — SeQure Quantum
Seminario: Hacia una regulación de la IA en Chile | 24 de abril de 2026