Índice de Preparación Criptográfica Cuántica para Empresas de Datos Médicos: Marco Teórico para Valoración de Riesgo en la Era Post-Cuántica

Andrea Camila*
AMLENTIA.org

13 de octubre de 2025

Resumen

El advenimiento de la computación cuántica plantea amenazas sin precedentes a los sistemas criptográficos tradicionales que protegen datos médicos sensibles. Este artículo desarrolla un Índice de Preparación Criptográfica Cuántica para empresas que gestionan información de salud, integrando dimensiones de inversión tecnológica, capacidad organizacional y cumplimiento regulatorio. A través de un modelo teórico fundamentado en teoría de decisiones y mecanismos de cooperación institucional, se cuantifica el nivel de preparación de las empresas frente a amenazas cuánticas futuras. El marco propuesto considera la paradoja temporal inherente a la protección de datos médicos: mientras que la amenaza cuántica es futura, las decisiones de inversión deben tomarse hoy para proteger información que debe permanecer confidencial durante décadas. Se demuestra que existe un equilibrio óptimo de inversión que balancea costos presentes contra riesgos futuros, y que este equilibrio depende críticamente de la estructura de gobernanza institucional y del horizonte temporal de protección requerido. El índice propuesto ofrece un instrumento cuantificable para evaluación de riesgo empresarial, decisiones de inversión tecnológica y diseño de política pública en seguridad de datos de salud. Los resultados sugieren que la preparación contra amenazas cuánticas debe conceptualizarse como problema de acción colectiva donde intervenciones regulatorias pueden mejorar coordinación y eficiencia sectorial.

*Correo electrónico: andrea.camila@AMLENTIA.org. Este trabajo fue desarrollado en colaboración con AMLENTIA.org

Palabras clave: Computación cuántica, criptografía post-cuántica, datos médicos, índice de preparación, gestión de riesgo
Códigos JEL: D81, I18, L51, O33

1. Introducción

La transición hacia sistemas de salud digitalizados ha generado concentraciones masivas de datos médicos en plataformas tecnológicas centralizadas. Estos repositorios de información clínica, genética y demográfica representan activos de enorme valor tanto para investigación científica como para medicina personalizada, pero simultáneamente constituyen objetivos críticos para amenazas de seguridad informática. La confidencialidad de datos médicos no es meramente una obligación legal sino un requisito fundamental para la confianza del paciente en el sistema de salud (**?**).

Los algoritmos criptográficos que actualmente protegen la transmisión y almacenamiento de datos médicos dependen de supuestos de complejidad computacional que serán invalidados por computadoras cuánticas suficientemente potentes. Los sistemas RSA y criptografía de curva elíptica, pilares de la seguridad digital contemporánea, son vulnerables a ataques mediante algoritmos cuánticos conocidos. Esta vulnerabilidad futura crea un problema de seguridad intertemporal sin precedentes en la historia de la criptografía (Bova et al., 2021).

La literatura sobre computación cuántica ha documentado extensamente las capacidades técnicas de estos sistemas emergentes para resolver problemas de optimización complejos en finanzas, energía y logística. Los estudios de Herman et al. (2022), Orús et al. (2019) y Islam et al. (2024) han demostrado aplicaciones prácticas en gestión de riesgo financiero, mientras que Mudhol (2024) y Aljaafari (2023) analizan implicaciones para análisis empresarial y optimización de negocios. Sin embargo, el análisis económico de las decisiones de inversión en protección criptográfica contra amenazas cuánticas permanece subdesarrollado, particularmente en el contexto de datos médicos donde los horizontes temporales de confidencialidad son extraordinariamente largos.

La contribución principal de este artículo consiste en desarrollar un marco teórico integrado para evaluar la preparación de empresas de datos médicos frente a amenazas criptográficas cuánticas. Construimos un Índice de Preparación Criptográfica Cuántica que agrega múltiples dimensiones de capacidad tecnológica, robustez organizacional y credibilidad regulatoria en una métrica cuantificable que puede informar decisiones de inversión, evaluación de riesgo y diseño de política pública.

El análisis se fundamenta en reconocer que la protección contra amenazas cuánti-

cas presenta características de problema de acción colectiva. Las empresas individuales enfrentan incentivos subóptimos para invertir en protección dado que los beneficios de seguridad robusta generan externalidades positivas sobre el ecosistema completo de salud digital, mientras que los costos son internalizados completamente (Holahan and Lubell, 2016). Esta estructura sugiere roles específicos para intervención regulatoria y mecanismos de coordinación sectorial.

El trabajo de de Jong (2022) propone una estrategia anticipatoria multidimensional para preparar la sociedad para tecnologías cuánticas, enfatizando desmistificación, contextualización, regulación flexible y diplomacia internacional. Complementariamente, Wolbring (2022) documenta la notable ausencia de consideraciones sociales en la literatura técnica sobre quantum computing, sugiriendo la necesidad de marcos analíticos que integren dimensiones tecnológicas, económicas y sociales. Este artículo responde a esta necesidad desarrollando un instrumento cuantitativo que conecta inversión tecnológica con objetivos sociales de privacidad y seguridad en salud.

La amenaza cuántica a la criptografía no es hipotética distante sino riesgo tangible que requiere acción inmediata. Como señalan Scholten et al. (2024), aunque los computadores cuánticos actuales no representan amenazas criptográficas inmediatas, las empresas serán capaces de realizar computaciones económicamente impactantes antes de alcanzar capacidades criptográficamente relevantes. Esta secuencia temporal genera una ventana de oportunidad para que empresas de datos médicos inviertan en protección post-cuántica antes de que las amenazas se materialicen.

El artículo se estructura como sigue. La sección dos revisa literatura relevante sobre computación cuántica en contextos empresariales, gestión de riesgo y teoría económica de cooperación institucional. La sección tres desarrolla el marco conceptual del Índice de Preparación Criptográfica Cuántica y sus componentes. La sección cuatro presenta el modelo teórico de decisión de inversión bajo incertidumbre temporal. La sección cinco analiza el problema de acción colectiva y roles de coordinación institucional. La sección seis discute implicaciones para política pública y regulación. La sección siete analiza mecanismos de implementación práctica del índice. La sección ocho concluye con reflexiones sobre extensiones futuras.

2. Revisión de Literatura

La literatura sobre aplicaciones empresariales de computación cuántica ha experimentado expansión considerable en años recientes. How and Cheah (2023) identifican oportunidades transformadoras en finanzas, salud y logística, junto con la

evolución de nuevos modelos de negocio como Quantum-as-a-Service. Sin embargo, también documentan que los algoritmos cuánticos amenazan fundamentalmente las medidas criptográficas existentes, creando imperativo para transición hacia criptografía resistente a ataques cuánticos.

En el dominio financiero, múltiples estudios han establecido aplicaciones prácticas de computación cuántica para gestión de riesgo y optimización. Herman et al. (2022) proveen revisión comprehensiva cubriendo modelado estocástico, optimización de portafolio y detección de fraude, argumentando que finanzas será el primer sector en beneficiarse de quantum computing en horizontes de corto, mediano y largo plazo. Islam et al. (2024) demuestran que computación cuántica ofrece ventajas competitivas en gestión de riesgo financiero a través de optimización de evaluación de riesgo y mejora significativa en modelos predictivos. Orús et al. (2019) analizan aplicaciones de quantum annealers para optimización de portafolios y credit scoring, mientras que Mugel et al. (2020) examinan casos de uso específicos en predicción de crashes financieros y optimización dinámica de portafolio.

Estas aplicaciones financieras son directamente relevantes para el contexto de datos médicos dado que la gestión de riesgo de seguridad informática comparte estructura analítica con gestión de riesgo financiero. Ambos dominios requieren cuantificación de probabilidades de eventos adversos de baja frecuencia pero alto impacto, y optimización de inversiones defensivas bajo restricciones presupuestarias.

La literatura sobre aplicaciones industriales más amplias de quantum computing documenta casos de uso en múltiples sectores. Quantum Technology and Application Consortium – QUTAC (2021) identifican 24 aplicaciones diferentes a través de consorcio representando industrias automotriz, química, farmacéutica y de seguros, estableciendo problemas de referencia y benchmarks para guiar comercialización. Gupta and Sharma (2023) analizan efectos en operaciones empresariales enfatizando seguridad mejorada junto con eficiencia y performance. Saltan and Hyrynsalmi (2022) proveen perspectiva empresarial enfatizando necesidad de entendimiento claro de desafíos y oportunidades para lograr impacto positivo.

Para análisis empresarial específicamente, Mudhol (2024) demuestran que quantum computing ofrece capacidades mejoradas de procesamiento de datos y algoritmos avanzados, identificando limitaciones técnicas, costos y accesibilidad como barreras principales. Taiwo et al. (2025) documentan potencial para reducir complejidad computacional hasta 90 por ciento en aplicaciones de business intelligence, mientras que Aljaafari (2023) identifican seis áreas críticas para adopción en comercio electrónico, incluyendo escalabilidad, desafíos regulatorios, costos y seguridad.

La literatura sobre aspectos sociales y éticos de tecnologías cuánticas es par-

ticularmente relevante para el contexto de datos médicos. de Jong (2022) proponen estrategia anticipatoria con cinco dimensiones: desmistificación de percepciones irrealistas, contextualización a través de ambiente socio-técnico facilitador, engajamiento de stakeholders, regulación con frameworks flexibles, y posicionamiento via diplomacia cuántica internacional. Wolbring (2022) proveen auditoría crítica documentando que solo 0.24 por ciento de 362,728 abstracts técnicos sobre quantum computing mencionan término social, y que frameworks de equidad, diversidad e inclusión están completamente ausentes, sugiriendo necesidad urgente de integrar consideraciones sociales en desarrollo tecnológico.

Wheatley Research Consultancy (2024) examinan implicaciones societales enfocando en seguridad de datos, privacidad y transformaciones económicas, mientras que de Wolf (2017) analizan impacto potencial en criptografía, optimización y simulación, proponiendo formas de mitigar riesgos. Coenen et al. (2022) presentan manifiesto para prevenir fiascos de implementación en interface ciencia-sociedad, identificando stumbling blocks y proponiendo recomendaciones para evitar que tecnologías cuánticas repitan problemas de tecnologías anteriores.

Un resultado crítico de Scholten et al. (2024) es que computadores cuánticos serán capaces de computaciones económicamente impactantes antes de alcanzar capacidades criptográficamente relevantes. Esta secuencia temporal tiene implicaciones importantes para estrategias de inversión empresarial, sugiriendo que beneficios de quantum computing en optimización y análisis de datos pueden materializarse antes que las amenazas criptográficas, potencialmente generando recursos para inversión en protección.

La teoría económica de cooperación institucional y acción colectiva provee fundamentos conceptuales para analizar decisiones de inversión en seguridad. Holahan and Lubell (2016) establecen que dilemas de acción colectiva ocurren cuando decisiones conjuntas resultan en outcomes socialmente indeseables, y que gobernanza efectiva requiere frameworks institucionales que alteren positivamente payoffs de cooperación. Dannenberg and Gallier (2020) revisan literatura experimental sobre elección endógena de instituciones para resolver dilemas de prisionero y juegos de bienes públicos, encontrando que instituciones mejoran cooperación cuando implementadas pero enfrentan barreras de costos, incentivos de free-riding y falta de aprendizaje.

Wooldridge (2020) introducen mechanism design para sistemas computacionales, donde diseñador crea reglas de juego para que, independiente de preferencias de participantes, objetivos del diseñador se alcancen cuando agentes actúan racionalmente. Crawford (2019) analizan experimentos sobre cognición, comunicación y

coordinación en relaciones, explorando cómo comunicación afecta cooperación. Moulin (2019) revisan resultados en división justa con foco en reglas con mejor potencial para implementación práctica.

En el contexto de salud específicamente, **?** analizan contratos incentive-compatible en healthcare que crean benchmarks alcanzables para resultados mejorados. Su análisis de diferentes formas de pago basado en valor sugiere que contratos bien diseñados pueden alinear incentivos para mejor cuidado y costos reducidos, relevante para diseño de mecanismos de incentivo para inversión en seguridad de datos.

Esta revisión identifica tres gaps principales en la literatura existente. Primero, mientras estudios técnicos documentan capacidades de quantum computing y amenazas criptográficas, existe análisis económico limitado de decisiones empresariales de inversión en protección post-cuántica. Segundo, aunque literatura sobre gestión de riesgo financiero es robusta, aplicación específica a riesgo de seguridad de datos médicos es escasa. Tercero, consideración de aspectos de acción colectiva y coordinación institucional en transición hacia criptografía post-cuántica está ausente. Este artículo contribuye llenando estos gaps mediante desarrollo de marco teórico integrado y construcción de índice cuantificable de preparación.

3. Construcción del Índice de Preparación Criptográfica Cuántica

El Índice de Preparación Criptográfica Cuántica para empresas de datos médicos se define como función que mapea características observables de la postura de seguridad de una empresa al espacio de preparación ante amenazas cuánticas futuras. La construcción del índice requiere especificar componentes fundamentales y relaciones entre ellos.

Sea I_{PCQ} el Índice de Preparación Criptográfica Cuántica para empresa i en periodo t. El índice agrega tres dimensiones principales: capacidad tecnológica de protección, robustez organizacional de implementación, y credibilidad de cumplimiento regulatorio. La forma funcional general es:

$$I_{PCQ} = g(C_T, R_O, C_R) \tag{1}$$

donde C_T representa capacidad tecnológica, R_O robustez organizacional, y C_R credibilidad regulatoria.

La capacidad tecnológica C_T cuantifica el nivel de adopción de soluciones criptográficas resistentes a ataques cuánticos. Esta dimensión incluye tanto implementa-

ción de algoritmos post-cuánticos como infraestructura para futuras actualizaciones. Formalmente:

$$C_T = \alpha_1 A_{PQ} + \alpha_2 I_{QKD} + \alpha_3 F_A \tag{2}$$

donde $A_{PQ} \in [0, 1]$ es el nivel de implementación de algoritmos post-cuánticos en sistemas de cifrado, transmisión y almacenamiento; $I_{QKD} \in [0, 1]$ representa inversión relativa en infraestructura de distribución cuántica de claves; y F_A es flexibilidad de arquitectura para adoptar nuevos estándares criptográficos.

Los parámetros $\alpha_1, \alpha_2, \alpha_3$ son ponderaciones con $\alpha_1+\alpha_2+\alpha_3 = 1$. En contexto de datos médicos donde información debe transmitirse frecuentemente entre instituciones, la ponderación α_1 sobre algoritmos post-cuánticos puede ser superior dado que representan solución más inmediatamente implementable que distribución cuántica de claves, aunque ambas son complementarias en arquitectura de seguridad robusta.

La robustez organizacional R_O captura capacidad institucional para implementar efectivamente tecnologías criptográficas avanzadas. Tecnología sin capacidad organizacional adecuada genera riesgos operacionales que comprometen seguridad efectiva. Esta dimensión se modela como:

$$R_O = \beta_1 Q_G + \beta_2 K_H + \beta_3 M_P \tag{3}$$

donde Q_G es calidad de gobernanza en gestión de seguridad de datos, K_H representa capital humano especializado medido por fracción de personal con formación en criptografía post-cuántica, y M_P captura madurez de procesos de seguridad incluyendo protocolos de respuesta a incidentes y auditorías regulares.

La credibilidad regulatoria C_R refleja historial de cumplimiento normativo y nivel de transparencia en reportes de seguridad. En sector de salud donde regulación es estricta y penalidades severas, esta dimensión adquiere peso sustancial:

$$C_R = \gamma_1 H_C + \gamma_2 N_T + \gamma_3 C_I \tag{4}$$

donde H_C es historial de cumplimiento medido por ausencia de violaciones previas, N_T es nivel de transparencia en reportes de auditorías y certificaciones, y C_I representa certificaciones independientes obtenidas de organismos especializados.

Integrando las tres dimensiones, el índice completo se especifica como función lineal ponderada:

$$I_{PCQ} = \omega_1 C_T + \omega_2 R_O + \omega_3 C_R \tag{5}$$

donde $\omega_1, \omega_2, \omega_3$ son ponderaciones que satisfacen $\omega_1 + \omega_2 + \omega_3 = 1$ y reflejan importancia relativa contextualmente determinada.

Una característica crítica del índice es que preparación efectiva exhibe complementariedades entre componentes. Alta capacidad tecnológica sin robustez organizacional puede resultar en implementación defectuosa que compromete seguridad. Para capturar estas complementariedades, definimos nivel de preparación efectiva como:

$$P_{EF} = I_{PCQ} + \eta(C_T \times R_O) - \lambda\sigma^2 \tag{6}$$

donde el término $\eta(C_T \times R_O)$ captura sinergia entre capacidad tecnológica y robustez organizacional, y $\lambda\sigma^2$ penaliza inconsistencia o alta varianza entre componentes del índice.

La varianza σ^2 mide dispersión entre dimensiones normalizadas. Empresa con muy alta capacidad tecnológica pero baja credibilidad regulatoria exhibe alta varianza, generando incertidumbre sobre sostenibilidad del compromiso con seguridad. El parámetro λ cuantifica intensidad con que el mercado o reguladores penalizan inconsistencia.

Para operacionalización empírica, cada componente requiere medición mediante datos observables. El nivel de implementación de algoritmos post-cuánticos A_{PQ} puede estimarse mediante auditorías técnicas de sistemas de cifrado. La inversión en infraestructura cuántica I_{QKD} se obtiene de estados financieros y presupuestos de inversión en TI. La flexibilidad arquitectural F_A requiere evaluación técnica de modularidad y capacidad de actualización de sistemas.

Los componentes organizacionales presentan mayor desafío de medición. Calidad de gobernanza Q_G puede aproximarse mediante índices de madurez de gestión de seguridad basados en frameworks establecidos. Capital humano K_H se cuantifica mediante análisis de credenciales y certificaciones de personal técnico. Madurez de procesos M_P puede evaluarse mediante frecuencia y profundidad de auditorías internas y externas.

La credibilidad regulatoria es más directamente observable. Historial de cumplimiento H_C se construye de registros públicos de violaciones y penalidades. Transparencia N_T se mide por frecuencia y detalle de reportes publicados. Certificaciones C_I son verificables directamente.

Un aspecto importante es normalización de componentes para comparabilidad. Dado que diferentes métricas tienen escalas naturales distintas, cada componente debe normalizarse al rango $[0, 1]$ antes de agregación. La normalización puede realizarse mediante transformación min-max o percentiles dentro de población relevante de empresas.

4. Modelo de Decisión de Inversión en Protección Post-Cuántica

Consideramos empresa que gestiona datos médicos y decide nivel óptimo de inversión en protección criptográfica post-cuántica. La empresa enfrenta trade-off intertemporal: inversión presente en protección genera costos inmediatos pero reduce riesgos futuros de violación de datos cuando computadoras cuánticas se desarrollen.

Sea $q \in [0, Q]$ el nivel de inversión en protección post-cuántica medido como fracción del presupuesto de TI. El costo de inversión en periodo presente es $C(q)$ con $C'(q) > 0$ y $C''(q) > 0$, reflejando costos marginales crecientes de implementación de soluciones criptográficas más sofisticadas.

El beneficio de la inversión se materializa en reducción de probabilidad de violación de datos en futuro cuando amenaza cuántica se concrete. Sea $p(q, t)$ la probabilidad de violación exitosa en periodo futuro t dado nivel de inversión q. Esta probabilidad decrece en q: $\partial p/\partial q < 0$, con rendimientos decrecientes $\partial^2 p/\partial q^2 > 0$.

La probabilidad también depende del tiempo hasta que computadoras cuánticas criptográficamente relevantes se desarrollen. Sea τ este horizonte temporal. Mientras τ es incierto, la empresa mantiene creencias sobre su distribución. La incertidumbre sobre τ introduce complejidad adicional en decisión de inversión.

El daño esperado de violación de datos incluye múltiples componentes: pérdidas legales por litigación y penalidades regulatorias L, deterioro de reputación que reduce demanda futura R, y costos de remediación M. El daño total esperado en periodo t es:

$$D(t) = p(q, t)[L + R(t) + M] \tag{7}$$

La empresa maximiza valor presente neto considerando costos de inversión presente contra beneficios de reducción de riesgo futuro. Con tasa de descuento δ, el problema de optimización es:

$$\max_q V(q) = -C(q) + \int_0^\infty e^{-\delta t}[D_0(t) - D(q, t)]f(\tau)d\tau \tag{8}$$

donde $D_0(t)$ es daño esperado sin inversión en protección post-cuántica, y $f(\tau)$ es densidad de probabilidad sobre horizonte temporal de amenaza cuántica.

La condición de primer orden caracteriza inversión óptima:

$$C'(q^*) = \int_0^\infty e^{-\delta t}\left[-\frac{\partial p}{\partial q}[L + R(t) + M]\right] f(\tau)d\tau \tag{9}$$

Esta condición establece que en óptimo, costo marginal de inversión adicional

iguala valor presente de reducción marginal en daño esperado. Varios resultados comparativos estáticos emergen de esta caracterización.

Primero, incrementos en daño potencial de violación aumentan inversión óptima. Empresas con mayor exposición legal o mayor valor reputacional invierten más en protección. Segundo, mayor incertidumbre sobre horizonte temporal de amenaza cuántica puede reducir o incrementar inversión dependiendo de actitud hacia riesgo y forma de función de probabilidad de violación.

Tercero, tasas de descuento más altas reducen inversión óptima al reducir valor presente de beneficios futuros. Este resultado sugiere que empresas con presiones financieras de corto plazo subinvertirán en protección post-cuántica, generando externalidades negativas sobre sistema completo de salud digital.

Para analizar rol de incertidumbre más formalmente, consideramos dos escenarios. En escenario determinista donde τ es conocido con certeza, inversión óptima resuelve:

$$C'(q_D^*) = e^{-\delta\tau}\left[-\frac{\partial p}{\partial q}[L + R(\tau) + M]\right] \tag{10}$$

Bajo incertidumbre con distribución $f(\tau)$ sobre horizonte temporal, inversión óptima satisface condición anterior con esperanza sobre τ. Si empresa es aversa a riesgo, puede invertir más bajo incertidumbre para protegerse contra posibilidad de que amenaza cuántica se materialice antes de lo esperado.

Un aspecto importante es heterogeneidad entre empresas en capacidad de inversión y exposición a riesgo. Empresas con mejor gobernanza enfrentan menores costos de implementación de soluciones criptográficas complejas debido a complementariedades organizacionales. Formalmente, el costo de inversión es $C(q, \theta)$ donde θ es parámetro de calidad institucional, con $\partial C/\partial\theta < 0$.

Esta heterogeneidad implica que en equilibrio observaremos dispersión en niveles de inversión entre empresas. Firmas con alta calidad institucional invertirán más en protección post-cuántica, mientras que empresas con gobernanza débil subinvertirán. Esta dispersión genera externalidades negativas: vulnerabilidad de empresas de baja preparación puede comprometer seguridad del ecosistema completo a través de interdependencias en redes de intercambio de datos médicos.

5. Problema de Acción Colectiva y Coordinación Institucional

La inversión en protección criptográfica post-cuántica en el sector de datos médicos exhibe características de problema de acción colectiva. Los beneficios de seguri-

dad robusta generan externalidades positivas sobre el ecosistema completo, mientras que costos son internalizados por empresas individuales. Esta estructura de incentivos puede resultar en subinversión agregada relativo al óptimo social.

Consideramos ecosistema con N empresas que intercambian datos médicos en red. Sea q_i el nivel de inversión de empresa i en protección post-cuántica. La probabilidad de que ecosistema completo experimente violación depende no solo de inversión propia sino también de inversión de empresas conectadas. Si empresa j tiene seguridad débil, puede servir como vector de ataque para comprometer datos que originaron en empresa i.

Modelamos esta interdependencia mediante función de riesgo sistémico. La probabilidad de que empresa i experimente violación es:

$$p_i(q_i, q_{-i}) = \phi(q_i) + \sum_{j \in N_i} \psi_{ij}(q_j) \tag{11}$$

donde $\phi(q_i)$ es riesgo directo que depende de inversión propia, y $\psi_{ij}(q_j)$ captura riesgo indirecto a través de conexión con empresa j. El conjunto N_i denota empresas directamente conectadas a i en red de intercambio de datos.

La función ϕ decrece en q_i mientras que ψ_{ij} decrece en q_j. La estructura precisa de estas funciones depende de arquitectura de red y protocolos de intercambio de datos. En red densamente conectada, externalidades de seguridad son más pronunciadas.

Empresa i maximiza utilidad privada:

$$U_i(q_i, q_{-i}) = B_i - C_i(q_i) - D_i p_i(q_i, q_{-i}) \tag{12}$$

donde B_i es beneficio base de operaciones, $C_i(q_i)$ es costo de inversión, y D_i es daño esperado de violación. La condición de mejor respuesta es:

$$C_i'(q_i^*) = -D_i \phi'(q_i^*) \tag{13}$$

Crucialmente, esta condición ignora efectos de inversión propia sobre riesgo de otras empresas. El óptimo social consideraría estos efectos externos. Un planificador social maximiza bienestar agregado:

$$W = \sum_{i=1}^{N} [B_i - C_i(q_i) - D_i p_i(q_i, q_{-i})] \tag{14}$$

La condición de primer orden para inversión socialmente óptima de empresa i

es:

$$C_i'(q_i^{SO}) = -D_i\phi'(q_i^{SO}) - \sum_{j\neq i} D_j\psi_{ji}'(q_i^{SO}) \tag{15}$$

El término adicional $\sum_{j\neq i} D_j\psi_{ji}'(q_i^{SO})$ captura beneficio marginal de reducir riesgo para empresas conectadas. Dado que $\psi_{ji}' < 0$, el lado derecho de la condición social excede al de equilibrio privado, implicando $q_i^{SO} > q_i^*$. Existe subinversión en equilibrio de mercado.

La magnitud de la brecha entre inversión social y privada depende de estructura de red y magnitud de daños. En redes densamente conectadas donde muchas empresas dependen de seguridad de cada nodo, externalidades son sustanciales. Cuando daños potenciales D_i son grandes, como en contexto de datos médicos sensibles, la subinversión puede ser severa.

Este análisis fundamenta roles para intervención institucional. Siguiendo marco de Holahan and Lubell (2016), dilemas de acción colectiva requieren gobernanza que altere payoffs para alinear incentivos privados con objetivos sociales. Varios mecanismos pueden implementarse.

Un mecanismo es establecimiento de estándar mínimo de inversión q_{min}. Empresas deben invertir al menos q_{min} para operar legalmente. El estándar óptimo balancea beneficios de mayor seguridad contra costos de compliance y potencial exclusión de empresas con baja capacidad. Si estándar es muy estricto, empresas pequeñas pueden ser forzadas a salir del mercado, reduciendo competencia.

Otro mecanismo es subsidios a inversión en protección post-cuántica. Un subsidio proporcional s reduce costo efectivo a $(1-s)C_i(q_i)$. El subsidio óptimo iguala externalidad marginal. Sin embargo, implementación requiere presupuesto gubernamental y genera costos de recaudación tributaria que deben considerarse en análisis de bienestar.

Un tercer mecanismo son esquemas de responsabilidad compartida donde empresas contribuyen a fondo común para compensar víctimas de violaciones de datos. Esto internaliza parcialmente externalidades al hacer que empresas con baja seguridad paguen por daños causados indirectamente. La efectividad depende de diseño específico del esquema de responsabilidad.

La literatura sobre elección de instituciones de Dannenberg and Gallier (2020) sugiere que implementación endógena de mecanismos de coordinación puede ser más efectiva que imposición exógena. Si empresas votan sobre adopción de estándar mínimo, aquellas cooperativas y con creencias optimistas sobre beneficios votarán a favor. Sin embargo, pueden existir barreras de free-riding y falta de aprendizaje que previenen adopción incluso cuando sería beneficiosa.

El diseño de mecanismo óptimo debe considerar heterogeneidad entre empresas. Wooldridge (2020) establecen que mechanism design efectivo crea reglas donde, independiente de preferencias privadas, comportamiento racional de participantes alcanza objetivos del diseñador. En contexto de protección post-cuántica, objetivo es lograr nivel agregado de inversión cercano al socialmente óptimo mientras respeta restricciones de participación de empresas heterogéneas.

6. Política Pública y Regulación para Seguridad Post-Cuántica

El análisis de secciones previas fundamenta roles específicos para política pública en transición hacia criptografía post-cuántica para datos médicos. Esta sección examina instrumentos regulatorios evaluados a través del marco del Índice de Preparación Criptográfica Cuántica.

Un primer instrumento es establecimiento de estándar mínimo de preparación. Empresas que gestionan datos médicos deberían alcanzar nivel mínimo I_{PCQ}^{min} para mantener licencia de operación. El nivel óptimo del estándar resuelve trade-off entre beneficios de mayor seguridad agregada y costos de compliance y reducción de competencia por exclusión de empresas de baja capacidad.

Formalmente, el bienestar social bajo estándar I_{PCQ}^{min} es:

$$W(I_{PCQ}^{min}) = \int_{I_{PCQ}^{min}}^{\bar{I}} \pi(I) dF(I) + B(I_{PCQ}^{min}) - L(I_{PCQ}^{min}) \tag{16}$$

donde $\pi(I)$ es beneficio privado de empresa con nivel de preparación I, $F(I)$ es distribución de preparación en población, B captura beneficios externos de seguridad agregada, y L representa pérdidas de variedad de servicios por salida de empresas.

El estándar óptimo I_{PCQ}^{min*} maximiza esta expresión. La caracterización precisa requiere estimación empírica de distribución de capacidades entre empresas y valoración de beneficios externos. Sin embargo, el análisis cualitativo sugiere que óptimo es interior: ni muy permisivo permitiendo empresas peligrosamente vulnerables, ni tan estricto que fuerza salida excesiva.

Un segundo instrumento son subsidios o incentivos fiscales. Un subsidio proporcional τ a inversión en protección post-cuántica reduce costo efectivo a $(1-\tau)C(q)$. El subsidio óptimo internaliza externalidad marginal de seguridad. Dado que empresas ignoran beneficios de su inversión sobre otras firmas en red, subsidio puede alinear incentivos privados con objetivos sociales.

El diseño óptimo del subsidio debe considerar heterogeneidad. Subsidios uniformes benefician desproporcionadamente a empresas grandes con mayor capacidad de absorción. Subsidios diferenciados por tamaño o capacidad pueden ser más efectivos pero generan complejidad administrativa. El análisis de **?** sobre contratos incentive-compatible en healthcare sugiere que diseño cuidadoso puede crear benchmarks alcanzables que mejoren outcomes sin generar gaming.

Un tercer instrumento importante es divulgación obligatoria de niveles de preparación. El Índice de Preparación Criptográfica Cuántica puede servir como base para sistema de calificación pública. Empresas serían evaluadas en dimensiones del índice y recibirían calificaciones que facilitan decisiones informadas de usuarios e instituciones médicas al seleccionar proveedores de servicios de gestión de datos.

La efectividad de divulgación depende de capacidad de usuarios para procesar información técnica compleja. Estudios sobre disclosure de riesgo sugieren que información debe presentarse de manera simple y comparable. Un sistema de calificación con categorías claras puede ser más efectivo que divulgación de métricas técnicas detalladas.

Un cuarto instrumento es certificación por terceros independientes. Agencias especializadas evaluarían implementación de protección post-cuántica y emitirían certificaciones verificables. Este mecanismo reduce costos de señalización al proveer información creíble sin requerir que cada empresa demuestre individualmente su nivel de seguridad. La efectividad requiere que agencias certificadoras sean verdaderamente independientes y posean expertise técnico suficiente.

El timing de intervención regulatoria es consideración crítica. Dada incertidumbre sobre horizonte temporal de amenaza cuántica, existe riesgo de procrastinación tanto por empresas como por reguladores. Mecanismos de compromiso como anuncios anticipados de estándares futuros pueden mitigar este problema. Por ejemplo, regulador podría anunciar hoy que en cinco años será requerido cierto nivel mínimo de protección post-cuántica, permitiendo a empresas planificar inversiones con anticipación.

La coordinación internacional es dimensión adicional importante. Como sugieren de Jong (2022), diplomacia cuántica internacional puede facilitar armonización de estándares entre jurisdicciones. Dado que datos médicos frecuentemente cruzan fronteras en investigación colaborativa, estándares armonizados reducen costos de compliance para empresas multinacionales.

Un aspecto final es educación y desarrollo de capacidad humana. Como documentan Aljaafari (2023), educación y entrenamiento son barreras críticas para adopción de tecnologías cuánticas. Programas de capacitación en criptografía post-cuántica

para profesionales de seguridad en salud pueden complementar instrumentos regulatorios directos, reduciendo costos de implementación y mejorando efectividad de protección.

7. Implementación Práctica del Índice

La utilidad del Índice de Preparación Criptográfica Cuántica depende críticamente de factibilidad de medición y cálculo en contextos reales. Esta sección discute aspectos prácticos de implementación incluyendo recolección de datos, metodología de cálculo y mecanismos de actualización.

Para medición de capacidad tecnológica, auditorías técnicas especializadas son necesarias. Auditores certificados evaluarían sistemas de cifrado, transmisión y almacenamiento para determinar nivel de implementación de algoritmos post-cuánticos. Esta evaluación requiere expertise en criptografía avanzada y acceso a documentación técnica detallada de arquitecturas de seguridad.

La inversión en infraestructura cuántica puede medirse mediante análisis de estados financieros y presupuestos de tecnología. Empresas reportarían gastos específicos en soluciones de distribución cuántica de claves y hardware relacionado. La flexibilidad arquitectural requiere evaluación de modularidad de sistemas y capacidad de integración de nuevos componentes criptográficos.

Para robustez organizacional, evaluación de gobernanza puede basarse en frameworks establecidos como COBIT o ISO 27001. Estos frameworks proveen criterios estructurados para valorar madurez de gestión de seguridad. Capital humano se cuantifica mediante inventario de credenciales y certificaciones de personal técnico, complementado con evaluación de programas de capacitación continua.

La madurez de procesos requiere revisión de documentación de procedimientos, análisis de frecuencia y profundidad de auditorías internas, y evaluación de capacidad de respuesta a incidentes mediante simulaciones o revisión de casos históricos.

Para credibilidad regulatoria, historial de cumplimiento se construye de registros públicos de violaciones, penalidades y acciones correctivas. Transparencia se mide por frecuencia de reportes publicados, nivel de detalle divulgado, y accesibilidad de información para stakeholders. Certificaciones son verificables directamente mediante confirmación con organismos emisores.

La agregación de componentes requiere decisiones sobre ponderaciones α, β, γ y ω. Estas ponderaciones pueden determinarse mediante varios métodos. Un enfoque es elicitar preferencias de expertos mediante técnicas como Analytic Hierarchy Process. Alternativamente, ponderaciones pueden calibrarse usando datos históricos

sobre relación entre componentes y outcomes de seguridad.

Un desafío importante es normalización de componentes con escalas naturales diferentes. Transformación min-max escala cada componente al rango $[0, 1]$ usando valores mínimo y máximo observados en población de referencia. Alternativamente, normalización por percentiles asigna valores basados en posición relativa en distribución poblacional.

La periodicidad de actualización del índice debe balancear necesidad de información actual contra costos de medición. Evaluación anual puede ser apropiada para mayoría de componentes, con actualizaciones más frecuentes para elementos que cambian rápidamente como certificaciones o inversiones en tecnología. Eventos significativos como violaciones de datos o cambios regulatorios mayores pueden desencadenar reevaluaciones extraordinarias.

Para facilitar comparabilidad entre empresas, estándares de medición deben estar claramente especificados y aplicados consistentemente. Un manual de procedimientos detallado para auditores puede asegurar que evaluaciones sean reproducibles y comparables. Calibración periódica entre auditores puede identificar y corregir inconsistencias en aplicación de criterios.

La presentación de resultados debe considerar audiencias diversas. Para reguladores, reportes técnicos detallados con desagregación completa de componentes son apropiados. Para usuarios y público general, visualizaciones simplificadas y calificaciones categóricas pueden ser más efectivas. Un dashboard interactivo que permita explorar diferentes niveles de detalle puede servir múltiples necesidades.

Un aspecto crítico es protección de información sensible. Aunque divulgación de niveles agregados de preparación es objetivo del índice, detalles técnicos específicos sobre implementaciones criptográficas no deben divulgarse públicamente dado que podrían facilitar ataques. El diseño del sistema de reporte debe balancear transparencia contra seguridad operacional.

8. Conclusión

Este artículo ha desarrollado un marco teórico integrado para evaluar preparación de empresas de datos médicos frente a amenazas criptográficas cuánticas emergentes. El Índice de Preparación Criptográfica Cuántica propuesto agrega dimensiones de capacidad tecnológica, robustez organizacional y credibilidad regulatoria en métrica cuantificable que puede informar decisiones empresariales, evaluación de riesgo y política pública.

El análisis ha establecido que inversión en protección post-cuántica enfrenta

trade-off intertemporal fundamental: costos presentes contra beneficios futuros de reducción de riesgo. La heterogeneidad entre empresas en capacidad institucional implica que en equilibrio de mercado observaremos dispersión sustancial en niveles de preparación, con empresas de alta calidad invirtiendo más que firmas con gobernanza débil.

Críticamente, el análisis ha demostrado que protección contra amenazas cuánticas presenta características de problema de acción colectiva. Externalidades positivas de seguridad robusta sobre ecosistema completo de salud digital no son completamente internalizadas por empresas individuales, resultando en subinversión agregada relativo al óptimo social. Esta estructura fundamenta roles para intervención institucional mediante estándares mínimos, subsidios, divulgación obligatoria y certificación por terceros.

Los resultados tienen relevancia práctica inmediata. Como establecen Scholten et al. (2024), aunque computadores cuánticos actuales no representan amenazas criptográficas inmediatas, empresas alcanzarán capacidades económicamente impactantes antes que criptográficamente relevantes. Esta secuencia temporal crea ventana de oportunidad para que empresas de datos médicos inviertan en protección antes de que amenazas se materialicen.

La implementación del índice propuesto enfrenta desafíos metodológicos incluyendo medición de componentes no observables, determinación de ponderaciones, y normalización de métricas dispares. Sin embargo, estos desafíos no son insuperables y marcos establecidos de evaluación de seguridad proveen fundamentos para desarrollo de protocolos de medición rigurosos.

Las extensiones futuras del trabajo deberían enfocarse en varias direcciones. Primero, validación empírica mediante aplicación del índice a muestra de empresas reales permitiría refinar especificación de componentes y calibrar ponderaciones. Segundo, desarrollo de modelos dinámicos que capturen evolución de preparación a lo largo del tiempo y efectos de aprendizaje organizacional enriquecería el análisis. Tercero, análisis de interdependencias en redes de intercambio de datos mediante teoría de grafos podría cuantificar externalidades con mayor precisión.

Cuarto, integración con marcos de evaluación de riesgo empresarial más amplios permitiría posicionar amenazas cuánticas en contexto de portafolio completo de riesgos que enfrentan empresas de salud digital. Quinto, análisis de economía política de adopción de regulación considerando intereses de stakeholders diversos proveería insights sobre factibilidad de implementación de diferentes instrumentos de política.

La transición hacia protección criptográfica post-cuántica en el sector de datos médicos representa desafío económico, tecnológico y social de magnitud considera-

ble. El marco desarrollado en este artículo establece fundamentos conceptuales para navegar esta transición de manera que balancee incentivos privados con objetivos sociales de privacidad y seguridad en sistema de salud digital. El Índice de Preparación Criptográfica Cuántica ofrece instrumento concreto para operacionalizar estos objetivos en contextos de política y práctica empresarial.

Referencias

Aljaafari, M. (2023). Quantum computing for social business optimization: a practitioner's perspective. *Soft Computing*.

Bova, F., Goldfarb, A., and Melko, R. G. (2021). Commercial applications of quantum computing. *EPJ Quantum Technology*, 8(1).

Coenen, C., Grinbaum, A., Grunwald, A., Milburn, C., and Vermaas, P. (2022). Quantum technologies and society: Towards a different spin. *NanoEthics*, 16(1):1–6.

Crawford, V. P. (2019). Experiments on cognition, communication, coordination, and cooperation in relationships. *Annual Review of Economics*, 11(1):167–191.

Dannenberg, A. and Gallier, C. (2020). The choice of institutions to solve cooperation problems: a survey of experimental research. *Experimental Economics*, 23(3):716–749.

de Jong, E. (2022). Own the unknown: An anticipatory approach to prepare society for the quantum age. *Digital Society*, 1(2).

de Wolf, R. (2017). The potential impact of quantum computers on society. *Ethics and Information Technology*, 19(4):271–276.

Gupta, S. and Sharma, V. (2023). Effects of quantum computing on businesses. In *2023 4th International Conference on Intelligent Engineering and Management (ICIEM)*, pages 1–6. IEEE.

Herman, D., Googin, C., Liu, X., Galda, A., Safro, I., Sun, Y., Pistoia, M., and Alexeev, Y. (2022). A survey of quantum computing for finance.

Holahan, R. and Lubell, M. (2016). Collective action theory. In *Handbook on Theories of Governance*. Edward Elgar Publishing.

How, M.-L. and Cheah, S.-M. (2023). Business renaissance: Opportunities and challenges at the dawn of the quantum computing era. *Businesses*, 3(4):585–605.

Islam, M. A., Hasan, S. K., Priya, S. A., Asha, A. I., and Islam, N. M. (2024). The impact of quantum computing on financial risk management: A business perspective. *International Journal For Multidisciplinary Research*, 6(5).

Moulin, H. (2019). Fair division in the internet age. *Annual Review of Economics*, 11(1):407–441.

Mudhol, A. C. (2024). Integrating quantum computing into business analytics: Opportunities and challenges. *International Journal of Innovative Science and Research Technology (IJISRT)*, pages 2451–2463.

Mugel, S., Lizaso, E., and Orús, R. (2020). Use cases of quantum optimization for finance.

Orús, R., Mugel, S., and Lizaso, E. (2019). Quantum computing for finance: Overview and prospects. *Reviews in Physics*, 4:100028.

Quantum Technology and Application Consortium – QUTAC (2021). Industry quantum computing applications. *EPJ Quantum Technology*.

Saltan, A. and Hyrynsalmi, S. (2022). The business perspective of quantum computing: An overview. In *ICSOB Companion*.

Scholten, T. L., Williams, C. J., Moody, D., Mosca, M., Hurley, W., Zeng, W. J., Troyer, M., and Gambetta, J. (2024). Assessing the benefits and risks of quantum computers.

Taiwo, I., Ogunbajo, A., and Abidola, A. Q. (2025). Quantum computing-enhanced ai systems for advanced business intelligence applications. *International Journal of Science and Research Archive*, 14(1):1839–1847.

Wheatley Research Consultancy (2024). Quantum shifts: The societal implications of quantum computing on security, privacy, and the economy.

Wolbring, G. (2022). Auditing the 'social' of quantum technologies: A scoping review. *Societies*, 12(2):41.

Wooldridge, M. (2020). Understanding mechanism design—part 1 of 3. *IEEE Intelligent Systems*, 35(4):110–111.