Indicador de Brecha de Accesibilidad Cripto-Cuántica en Poblaciones Vulnerables: Un Modelo Teórico de Costos y Seguridad de Datos

Andrea Camila*
AMLENTIA.org

Resumen

La emergencia de la criptografía cuántica como tecnología de protección de datos genera nuevas brechas de accesibilidad económica que afectan desproporcionadamente a poblaciones vulnerables. Este artículo desarrolla un indicador teórico que mide la brecha entre el costo de implementación de protección cripto-cuántica y la capacidad económica de individuos en situación de pobreza para acceder a dicha protección. A través de un modelo algebraico, se construye el Índice de Vulnerabilidad Cripto-Económica (IVCE) que integra tres dimensiones: costos de transición tecnológica, nivel de ingresos de la población objetivo, y valor económico de los datos personales en riesgo. El modelo demuestra que la asimetría en el acceso a tecnologías de protección cuántica amplifica la vulnerabilidad de datos de poblaciones de bajos ingresos, creando una nueva forma de desigualdad digital con consecuencias económicas medibles. Los resultados teóricos sugieren que sin intervención de política pública, la brecha de protección cripto-cuántica puede perpetuar ciclos de vulnerabilidad económica en sectores marginados, donde el costo de no proteger datos sensibles supera significativamente la capacidad de pago por tecnologías de seguridad avanzadas.

Palabras clave: Criptografía cuántica, vulnerabilidad económica, brecha digital, protección de datos, poblaciones de bajos ingresos
Códigos JEL: D63, I32, O33, D82

*Correspondencia: andrea.camila@AMLENTIA.org. Este trabajo fue desarrollado en colaboración con AMLENTIA.org, organización dedicada a la investigación en economía de tecnologías emergentes y equidad digital.

1. Introducción

La transición hacia sistemas de comunicación protegidos por criptografía cuántica representa un punto de inflexión en la arquitectura de seguridad digital global. Mientras la computación cuántica amenaza los sistemas criptográficos convencionales, las tecnologías cuánticas ofrecen simultáneamente soluciones de protección fundamentadas en leyes de la física cuántica (Wheatley Research Consultancy, 2024). Sin embargo, esta revolución tecnológica no se distribuye uniformemente entre diferentes estratos socioeconómicos, generando una nueva dimensión de desigualdad que este artículo examina sistemáticamente.

La literatura sobre impactos societales de tecnologías cuánticas ha identificado tres áreas críticas de transformación: seguridad de datos mediante criptografía quantum-resistant, capacidades ampliadas de procesamiento de información, y transformaciones económicas que afectarán mercados laborales e industrias (Wheatley Research Consultancy, 2024). No obstante, investigaciones recientes demuestran una ausencia notable de consideraciones sobre equidad, diversidad e inclusión en el desarrollo de tecnologías cuánticas (Wolbring, 2022). Esta omisión resulta particularmente preocupante cuando se considera que tecnologías emergentes han mostrado históricamente patrones de adopción que benefician desproporcionadamente a segmentos de mayores ingresos, generando brechas persistentes de acceso (López-Claros, 2011).

La justificación de este estudio radica en una paradoja observable en mercados de protección de datos: precisamente aquellos individuos que enfrentan mayor riesgo relativo por la exposición de sus datos personales son quienes tienen menor capacidad económica para adquirir tecnologías avanzadas de protección. Los datos personales de individuos en situación de pobreza pueden ser críticos para su acceso a servicios financieros, programas de transferencias condicionadas, sistemas de identificación digital, y oportunidades laborales en economías digitalizadas. La compromisión de estos datos puede tener consecuencias económicas devastadoras para poblaciones vulnerables, generando exclusión de servicios esenciales.

Investigaciones sobre tecnología y desigualdad han documentado cómo nuevas tecnologías presentan riesgos significativos de desempleo y aumento de desigualdad de riqueza, especialmente para trabajadores de baja calificación (United Nations, 2018; Dachs, 2017). En el contexto de tecnologías cuánticas, la literatura emergente enfatiza la necesidad de democratizar el acceso para garantir que beneficien a toda la humanidad y no exacerben desigualdades existentes (Troyer et al., 2024). Sin embargo, existe una brecha crítica en el desarrollo de marcos analíticos que permitan cuantificar y medir estas brechas de accesibilidad específicamente en el contexto de protección cripto-cuántica.

El objetivo central de este artículo es desarrollar un marco teórico que permita cuantificar la brecha de accesibilidad cripto-cuántica mediante la construcción de un indicador

económico específico: el Índice de Vulnerabilidad Cripto-Económica (IVCE). Este índice integra tres componentes fundamentales que interactúan de manera no lineal: primero, el costo marginal de transición desde sistemas de protección clásicos hacia sistemas cuánticos; segundo, la capacidad de pago de poblaciones en diferentes percentiles de distribución de ingresos; y tercero, el valor económico esperado de los datos en riesgo para cada segmento poblacional. La hipótesis central sostiene que existe una relación inversa entre vulnerabilidad económica y acceso a protección cripto-cuántica, generando una externalidad negativa que amplifica desigualdades preexistentes.

Metodológicamente, este trabajo adopta un enfoque teórico-algebraico que permite abstraer los principios económicos fundamentales sin recurrir a simulaciones empíricas o datos específicos de países particulares. Esta elección metodológica se justifica porque las tecnologías cuánticas se encuentran en fases tempranas de despliegue comercial, limitando la disponibilidad de datos robustos, y porque el objetivo es desarrollar un marco conceptual generalizable aplicable a diferentes contextos institucionales y geográficos. Además, marcos antecipatorios son necesarios para preparar a la sociedad antes de que estas tecnologías alcancen madurez comercial completa (de Jong, 2022).

La estructura del artículo se organiza de la siguiente manera: la sección 2 establece el marco teórico conceptual, revisando literatura relevante sobre economía de tecnologías cuánticas y desigualdad digital; la sección 3 desarrolla formalmente el modelo algebraico del IVCE, especificando sus componentes y propiedades matemáticas; la sección 4 analiza las implicaciones del modelo para poblaciones vulnerables; la sección 5 presenta una discusión crítica sobre limitaciones y extensiones posibles; finalmente, la sección 6 ofrece conclusiones y recomendaciones de política pública.

2. Marco Teórico y Conceptual

El desarrollo de tecnologías cuánticas plantea cuestiones éticas, legales, sociales y de política pública que requieren abordaje interdisciplinario (Kop, 2023). En particular, la criptografía cuántica y las comunicaciones cuánticas representan aplicaciones de primera generación con implicaciones inmediatas para seguridad de datos (Young et al., 2024). La literatura sobre impactos societales de estas tecnologías identifica tensiones fundamentales entre objetivos sociales que requieren balances cuidadosos entre riesgos y beneficios (Coenen et al., 2022).

Desde una perspectiva de economía de la innovación, las tecnologías emergentes presentan patrones característicos de difusión donde adopción temprana se concentra en segmentos con mayor capacidad económica y mayor alfabetización tecnológica (López-Claros, 2011). Este patrón ha sido documentado extensamente en contextos de automatización y

digitalización, donde los beneficios tienden a distribuirse desigualmente, generando preocupaciones sobre exacerbación de desigualdades existentes (United Nations, 2018). En el caso específico de tecnologías cuánticas, existe reconocimiento creciente de que su desarrollo debe considerar explícitamente dimensiones de equidad y acceso para evitar reproducir errores de tecnologías anteriores (Troyer et al., 2024).

La brecha digital, tradicionalmente conceptualizada en términos de acceso a infraestructura de internet y dispositivos, requiere actualización para incorporar dimensiones de seguridad y protección de datos (Bulatova et al., 2023). Investigaciones recientes sobre desigualdad digital argumentan que las brechas contemporáneas no se limitan a conectividad básica sino que abarcan capacidades diferenciadas para proteger información personal, acceder a servicios digitales seguros, y participar en economías digitales sin exposición desproporcionada a riesgos (Bulatova et al., 2023). En este contexto, la protección criptocuántica puede entenderse como un nuevo nivel de brecha digital donde capacidad de proteger infraestructura digital contra amenazas cuánticas avanzadas se distribuye desigualmente entre poblaciones.

La economía de tecnologías disruptivas identifica que procesos de transformación tecnológica generan desajustes de habilidades que afectan desproporcionadamente a trabajadores de baja calificación y bajos ingresos (Cukier, 2019). Evidencia empírica de contextos de automatización muestra que grupos más vulnerables enfrentan mayores riesgos cuando tecnologías transforman estructuras laborales (Katz et al., 2021). Aunque estas investigaciones se han centrado principalmente en impactos laborales directos, sus hallazgos son relevantes para comprender cómo brechas de acceso a tecnologías de protección pueden amplificar vulnerabilidades económicas existentes.

La teoría sobre impacto de nuevas tecnologías en mercado laboral sugiere que innovación es fundamentalmente labor-friendly en el largo plazo, destruyendo pero también creando empleos (Dachs, 2017). Sin embargo, los costos de esta transición se distribuyen desigualmente debido a la naturaleza skill-biased del cambio tecnológico, donde trabajadores de baja calificación enfrentan mayores riesgos durante períodos de ajuste. Extrapolando este razonamiento al contexto de protección de datos, individuos con menores recursos enfrentan períodos de vulnerabilidad elevada durante transiciones tecnológicas hacia nuevos estándares de seguridad que no pueden costear.

Desde la perspectiva de tecnología y derechos humanos, investigaciones recientes argumentan que desarrollo de tecnologías cuánticas debe considerar explícitamente su impacto sobre derechos fundamentales, incluyendo privacidad y seguridad de información personal (Krishnamurthy, 2022). El marco de derechos humanos sugiere que acceso a protección básica de datos personales podría conceptualizarse como derecho habilitante que facilita ejercicio de otros derechos en sociedades digitalizadas. Esta perspectiva normativa

refuerza la importancia de desarrollar indicadores que midan brechas de accesibilidad a tecnologías de protección.

La literatura sobre ética de tecnologías cuánticas enfatiza necesidad de frameworks comprehensivos que integren consideraciones de equidad y justicia distributiva en el desarrollo tecnológico (Damayanti, 2024). Estos marcos normativos argumentan que estrategias de desarrollo tecnológico deben priorizar cuestiones éticas desde fases tempranas, requiriendo esfuerzos coordinados entre múltiples stakeholders incluyendo sectores de tecnología, política y gobernanza. En particular, se identifica que obstáculos principales para desarrollo equitativo incluyen preocupaciones sobre privacidad, seguridad, y potencial para sesgos sistémicos en acceso a beneficios tecnológicos.

Investigaciones sobre preparación societal para era cuántica proponen estrategias anticipatorias con múltiples dimensiones: desmistificación de percepciones tecnológicas, contextualización mediante ambientes sociotécnicos facilitadores, engajamiento de sociedad civil, regulación flexible, y diplomacia internacional (de Jong, 2022). Este enfoque anticipatorio reconoce que intervenciones proactivas son necesarias para evitar que brechas de accesibilidad se consoliden durante fases tempranas de desarrollo tecnológico.

Finalmente, el análisis crítico de tecnologías cuánticas desde perspectivas de ciencias sociales revela una ausencia significativa de consideraciones sobre poblaciones marginalizadas y frameworks de equidad en la literatura técnica (Wolbring, 2022). De aproximadamente 363,000 abstracts técnicos analizados, menos de 0.24 por ciento mencionan aspectos sociales, y frameworks de equidad, diversidad e inclusión están completamente ausentes. Esta laguna en la literatura técnica subraya la urgencia de desarrollar marcos analíticos que expliciten dimensiones distributivas de tecnologías cuánticas emergentes.

3. Construcción del Índice de Vulnerabilidad Cripto-Económica

Esta sección desarrolla formalmente el Índice de Vulnerabilidad Cripto-Económica (IVCE), un indicador teórico que captura la brecha entre necesidad de protección criptocuántica y capacidad económica de acceso a dicha protección para poblaciones vulnerables. El modelo se construye de manera algebraica, identificando componentes fundamentales y sus interacciones.

3.1. Componentes del Modelo

Sea P una población heterogénea caracterizada por una distribución de ingresos continua. Para cualquier individuo i en esta población, definimos su nivel de ingreso como y_i,

donde $y_i \in [y_{min}, y_{max}]$. Sin pérdida de generalidad, ordenamos la población de manera que $y_1 \leq y_2 \leq ... \leq y_n$.

El costo de transición hacia protección cripto-cuántica para el individuo i se denota como C_i^Q. Este costo incluye múltiples componentes: adquisición de hardware compatible, suscripción a servicios de distribución cuántica de claves, capacitación necesaria para uso efectivo, y costos de oportunidad asociados a la migración de sistemas. Modelamos este costo como función de dos parámetros fundamentales:

$$C_i^Q = C_0 + \theta \cdot f(y_i) \tag{1}$$

donde $C_0 > 0$ representa el costo fijo mínimo de acceso, independiente del nivel de ingreso, $\theta > 0$ es un parámetro de escala, y $f(y_i)$ es una función creciente que captura cómo ciertos componentes del costo pueden variar con el ingreso del individuo. Para poblaciones vulnerables donde y_i es bajo, el costo fijo C_0 domina la expresión.

El valor económico de los datos en riesgo para el individuo i se denota como V_i^D. Este valor no refleja necesariamente el precio de mercado de los datos, sino el costo económico esperado que el individuo enfrentaría si sus datos fueran comprometidos. Formalmente:

$$V_i^D = \sum_{j=1}^{m} p_j \cdot L_{ij} \tag{2}$$

donde p_j representa la probabilidad de que ocurra el evento de compromiso j (fraude financiero, robo de identidad, exclusión de servicios, etc.), y L_{ij} es la pérdida económica asociada al evento j para el individuo i. Para poblaciones vulnerables, aunque las pérdidas absolutas puedan ser menores en términos monetarios, su impacto relativo sobre el bienestar puede ser desproporcionadamente alto.

La capacidad de pago del individuo i se define como la fracción de ingreso disponible que podría, en principio, destinarse a protección de datos sin comprometer necesidades básicas. Sea α_i esta fracción, donde:

$$\alpha_i = \text{máx}\left\{0, \frac{y_i - y_{subsist}}{y_i}\right\} \tag{3}$$

siendo $y_{subsist}$ el nivel de ingreso de subsistencia, que representa el mínimo necesario para cubrir necesidades básicas. Para individuos con $y_i \leq y_{subsist}$, se tiene $\alpha_i = 0$, indicando ausencia total de capacidad de pago para tecnologías de protección.

3.2. Formulación del Indicador

El IVCE para el individuo i se construye como la razón entre la necesidad de protección (medida por el valor de datos en riesgo) y la capacidad efectiva de adquirir protección

cripto-cuántica. Formalmente:

$$IVCE_i = \frac{V_i^D}{C_i^Q} \cdot \frac{1}{\alpha_i + \epsilon} \tag{4}$$

donde $\epsilon > 0$ es una constante pequeña que previene divisiones por cero cuando $\alpha_i = 0$. Esta especificación captura una intuición económica fundamental: la vulnerabilidad es alta cuando el valor de lo que está en riesgo es elevado, el costo de protección es alto, y la capacidad de pago es baja.

Alternativamente, podemos expresar el IVCE en forma logarítmica para facilitar interpretaciones de elasticidad:

$$\ln(IVCE_i) = \ln(V_i^D) - \ln(C_i^Q) - \ln(\alpha_i + \epsilon) \tag{5}$$

Esta formulación permite descomponer aditivamente las tres fuentes de vulnerabilidad. Para poblaciones en el percentil más bajo de ingresos, donde $\alpha_i \approx 0$, el tercer término $-\ln(\epsilon)$ domina, generando valores altos del índice.

Para obtener un indicador agregado a nivel poblacional, definimos:

$$IVCE_{agg} = \frac{1}{n} \sum_{i=1}^{n} w_i \cdot IVCE_i \tag{6}$$

donde w_i son ponderadores que pueden asignar mayor peso a segmentos más vulnerables. Una especificación natural sería $w_i = 1/y_i$, dando mayor importancia a individuos de menores ingresos en el cálculo del indicador agregado.

3.3. Propiedades Teóricas del Indicador

El IVCE satisface varias propiedades deseables para un indicador de vulnerabilidad económica. Primero, es monótono creciente en V_i^D: aumentos en el valor de datos en riesgo, manteniendo todo lo demás constante, incrementan la vulnerabilidad medida. Segundo, es monótono decreciente en α_i: mayor capacidad de pago reduce la vulnerabilidad. Tercero, presenta no linealidad en los efectos de interacción: el impacto de un aumento en C_i^Q sobre el IVCE es mayor cuando α_i es bajo.

Matemáticamente, podemos derivar la elasticidad del IVCE respecto al ingreso. Definamos:

$$\eta_{IVCE,y} = \frac{\partial \ln(IVCE_i)}{\partial \ln(y_i)} = \eta_{V,y} - \eta_{C,y} - \eta_{\alpha,y} \tag{7}$$

donde $\eta_{V,y}$, $\eta_{C,y}$, y $\eta_{\alpha,y}$ representan las elasticidades de V_i^D, C_i^Q, y α_i respecto al ingreso, respectivamente. Para poblaciones de bajos ingresos cercanas al nivel de subsistencia,

esperamos que $\eta_{\alpha,y}$ sea alta, lo que implicaría que el IVCE es especialmente sensible a cambios en ingreso en rangos bajos de la distribución.

Un resultado teórico relevante surge al analizar la brecha de vulnerabilidad entre diferentes percentiles de ingreso. Sea $IVCE_p$ el valor del índice para individuos en el percentil p de la distribución de ingresos. Podemos definir la brecha relativa de vulnerabilidad entre el percentil bajo p_L y el percentil alto p_H como:

$$\Delta IVCE = \frac{IVCE_{p_L} - IVCE_{p_H}}{IVCE_{p_H}} \tag{8}$$

El modelo predice que $\Delta IVCE > 0$ y potencialmente muy grande cuando la tecnología cripto-cuántica tiene costos fijos altos relativos a la capacidad de pago de segmentos vulnerables.

4. Análisis de Costos y Accesibilidad para Poblaciones Vulnerables

La aplicación del IVCE a poblaciones vulnerables revela dinámicas económicas específicas que exacerban la brecha de protección cripto-cuántica. Esta sección analiza tres dimensiones críticas: la estructura de costos de transición tecnológica, las barreras de acceso económico, y las consecuencias de la no protección.

4.1. Estructura de Costos y Distribución del Ingreso

Los costos asociados a la adopción de tecnologías cripto-cuánticas presentan una estructura particular donde componentes fijos dominan sobre componentes variables. Podemos descomponer C_i^Q en tres categorías principales: costos de infraestructura física (C^{inf}), costos de servicios recurrentes (C^{serv}), y costos de aprendizaje y adaptación (C^{adapt}). Formalmente:

$$C_i^Q = C^{inf} + C^{serv}(T) + C^{adapt}(h_i) \tag{9}$$

donde T representa el horizonte temporal de uso previsto y h_i el capital humano del individuo i. Para poblaciones vulnerables, cada componente presenta desafíos específicos. El costo de infraestructura C^{inf} es esencialmente fijo e independiente del nivel de ingreso, creando una barrera de entrada absoluta. El costo de servicios presenta umbrales mínimos de contratación que pueden exceder la capacidad de pago de individuos en percentiles bajos de ingresos.

La relación entre estos costos y la distribución del ingreso se vuelve crítica al considerar que para un individuo en el percentil p de ingresos, el ratio costo-ingreso es:

$$R_p = \frac{C_p^Q}{y_p} \tag{10}$$

Si la distribución de ingresos presenta alta concentración en percentiles bajos (como es típico en economías con alta desigualdad), entonces R_p puede ser prohibitivamente alto para una fracción sustancial de la población. Específicamente, si $y_p < C^{inf}/\tau$ donde τ es la fracción máxima de ingreso que un individuo racionalmente destinaría a protección de datos, entonces el acceso resulta económicamente inviable.

Esta barrera de acceso es particularmente problemática en contextos donde evidencia empírica sugiere que trabajadores de baja calificación y bajos ingresos enfrentan riesgos desproporcionados durante transiciones tecnológicas (Katz et al., 2021; Yolusever, 2025). La combinación de mayor vulnerabilidad con menor capacidad de acceso a protección genera una dinámica que puede exacerbar ciclos de exclusión económica.

4.2. Dinámica Temporal y Persistencia de la Brecha

La brecha de accesibilidad no es estática sino que evoluciona temporalmente de manera que puede amplificar o atenuar desigualdades iniciales. Modelamos la evolución del IVCE en el tiempo como:

$$IVCE_i(t) = IVCE_i(0) \cdot \exp\left(\beta_V \cdot t - \beta_C \cdot t - \beta_\alpha \cdot t\right) \tag{11}$$

donde β_V, β_C, y β_α representan las tasas de crecimiento del valor de datos en riesgo, reducción de costos tecnológicos, y mejora en capacidad de pago, respectivamente. Para que la brecha se reduzca en el tiempo, se requiere que:

$$\beta_C + \beta_\alpha > \beta_V \tag{12}$$

es decir, que la combinación de abaratamiento tecnológico y crecimiento económico supere el incremento en el valor de los datos en riesgo. Sin embargo, la evidencia histórica de difusión de tecnologías de seguridad sugiere que β_C es típicamente bajo en fases tempranas de adopción, precisamente cuando las amenazas a sistemas convencionales (y por tanto β_V) son más altas. Esto genera una ventana temporal crítica donde la vulnerabilidad de poblaciones de bajos ingresos puede aumentar antes de que los beneficios de economías de escala se materialicen.

4.3. Valor de Datos en Riesgo y Poblaciones Vulnerables

Un aspecto contraintuitivo del modelo es que el valor económico de datos en riesgo V_i^D puede ser proporcionalmente mayor para individuos vulnerables, incluso si su valor absoluto es menor. Esto se debe a que las pérdidas derivadas de compromiso de datos pueden representar una fracción más grande del patrimonio total y pueden tener consecuencias más severas en términos de acceso a servicios esenciales.

Consideremos un individuo vulnerable que depende de transferencias condicionadas de programas sociales. Si sus datos biométricos o de geolocalización son comprometidos de manera que le impiden verificar cumplimiento de condicionalidades, la pérdida esperada es:

$$L_i^{social} = \gamma \cdot T_{social} \tag{13}$$

donde γ es la probabilidad de exclusión del programa por compromiso de datos, y T_{social} es el valor presente de transferencias futuras. Para un individuo en extrema pobreza, T_{social} puede representar una fracción sustancial del ingreso total esperado, haciendo que V_i^D sea alto en términos relativos. Sin embargo, este alto valor no se traduce en capacidad de pago para tecnologías de protección, generando la paradoja de mayor necesidad con menor acceso.

5. Implicaciones Económicas y Sociales del Modelo

Las implicaciones derivadas del modelo IVCE trascienden el ámbito puramente técnico de adopción tecnológica para situarse en el centro de debates sobre equidad digital y justicia distributiva en la era de tecnologías cuánticas emergentes. Esta sección analiza tres conjuntos de implicaciones: efectos sobre desigualdad económica, externalidades sistémicas, y dimensiones de política pública.

5.1. Amplificación de Desigualdades Preexistentes

El modelo sugiere que la brecha de accesibilidad cripto-cuántica opera como un mecanismo de amplificación de desigualdades económicas preexistentes a través de varios canales. Primero, genera divergencia en acumulación de capital informacional: individuos con capacidad de proteger sus datos pueden acumular historiales digitales más completos y confiables, lo cual tiene valor económico en mercados laborales, crediticios y de seguros. Poblaciones vulnerables sin acceso a protección adecuada enfrentan mayor probabilidad de contaminación o pérdida de estos activos informacionales.

Esta dinámica es particularmente relevante en economías digitales donde automatización e inteligencia artificial están remodelando mercados laborales (Kuban State Agrarian University et al., 2025; Yolusever, 2025). Investigaciones recientes demuestran que automatización de profesiones de baja calificación puede sustituir hasta 98 por ciento de esos empleos, profundizando desigualdades en acceso a recursos y tecnologías (Kuban State Agrarian University et al., 2025). En este contexto, la incapacidad de proteger datos personales puede limitar aún más oportunidades económicas para poblaciones vulnerables en economías digitalizadas.

Segundo, crea asimetrías en capacidad de participación en economías digitales emergentes. Si ciertos servicios financieros, laborales o gubernamentales migran hacia plataformas que requieren protección cripto-cuántica como condición de participación (por motivos de seguridad sistémica), individuos sin capacidad de acceso enfrentan exclusión efectiva. Esta exclusión tiene costos económicos medibles en términos de oportunidades perdidas, especialmente considerando que las brechas digitales contemporáneas ya limitan participación económica de poblaciones vulnerables (Bulatova et al., 2023).

Tercero, modifica la distribución de riesgos de manera regresiva. En ausencia de intervención, el riesgo de compromiso de datos se concentra desproporcionadamente en segmentos de bajos ingresos, quienes simultáneamente tienen menor capacidad de absorber las consecuencias económicas negativas de tales compromisos. Esto contrasta con principios de distribución eficiente de riesgos que sugerirían que agentes con mayor capacidad de soportar pérdidas deberían asumir mayor exposición.

5.2. Externalidades y Efectos Sistémicos

La vulnerabilidad concentrada en segmentos poblacionales específicos genera externalidades negativas que afectan al sistema económico en su conjunto. Si una fracción significativa de la población mantiene datos sin protección cuántica adecuada, se crean vectores de ataque que pueden comprometer la seguridad de redes completas. Esta externalidad es particularmente relevante en sistemas donde los datos de múltiples individuos están interconectados, como registros de salud pública, sistemas de votación electrónica, o infraestructuras de identificación digital.

Modelamos esta externalidad como una función de la proporción de población vulnerable π_v:

$$E_{sist}(\pi_v) = \kappa \cdot \pi_v \cdot (1 - \pi_v) \tag{14}$$

donde $\kappa > 0$ es un parámetro que captura la intensidad de interconexión del sistema. Esta especificación refleja que las externalidades son máximas cuando hay una división

aproximadamente equilibrada entre población protegida y vulnerable, creando interfaces de vulnerabilidad extensas. El costo social total de estas externalidades puede exceder significativamente la suma de costos privados de protección, justificando intervención colectiva.

Adicionalmente, la persistencia de brechas de protección puede generar efectos de histéresis en desarrollo tecnológico. Si los desarrolladores de servicios digitales perciben que una fracción de usuarios no puede acceder a protección cuántica, pueden tener incentivos para mantener compatibilidad con estándares criptográficos clásicos, retrasando la transición completa del ecosistema y prolongando ventanas de vulnerabilidad para todos los participantes.

5.3. Dimensiones de Política Pública

El análisis del IVCE sugiere múltiples puntos de intervención de política pública para reducir la brecha de vulnerabilidad. La literatura sobre tecnologías cuánticas y sociedad enfatiza que desarrollo responsable requiere consideración explícita de implicaciones éticas, legales y sociales desde fases tempranas (Kop, 2023; Troyer et al., 2024). Desde una perspectiva teórica, estas intervenciones pueden clasificarse según el componente del índice sobre el cual operan: reducción de costos de acceso, incremento de capacidad de pago, o modificación del valor de datos en riesgo.

Las políticas orientadas a reducción de costos incluyen subsidios directos para adquisición de tecnologías cripto-cuánticas por parte de poblaciones vulnerables, mandatos de provisión de servicios básicos de protección como parte de infraestructura pública, o regulaciones que requieran interoperabilidad entre sistemas cuánticos y clásicos durante períodos de transición. El marco de democratización del acceso propuesto en la literatura sugiere que infraestructura digital debe considerarse como bien público esencial (Troyer et al., 2024).

Las intervenciones sobre capacidad de pago incluyen transferencias monetarias específicamente condicionadas a adquisición de protección de datos, o esquemas de seguros colectivos que distribuyan el costo de protección a través de mecanismos de riesgo compartido. Estas aproximaciones tienen la ventaja de preservar elección individual mientras mejoran restricciones presupuestarias, pero requieren que los individuos valoren correctamente los beneficios de protección, lo cual puede no ocurrir si existen problemas de información o sesgos cognitivos.

Finalmente, políticas que modifiquen directamente el valor de datos en riesgo incluyen regulaciones sobre uso y comercialización de datos personales que reduzcan el incentivo económico para actores maliciosos de comprometer información de poblaciones vulnerables. Desde una perspectiva de derechos humanos, estas regulaciones pueden con-

ceptualizarse como mecanismos para garantizar protección básica de datos como derecho fundamental (Krishnamurthy, 2022).

El modelo también sugiere que la combinación óptima de políticas puede depender críticamente de la distribución del ingreso en la economía. En contextos de alta desigualdad donde una fracción muy grande de la población se encuentra bajo el umbral de acceso económico, intervenciones de provisión pública universal pueden ser más eficientes que esquemas selectivos. Marcos antecipatorios sugieren que estas intervenciones deben implementarse proactivamente antes de que brechas se consoliden (de Jong, 2022).

6. Discusión

El marco teórico desarrollado en este artículo abre múltiples líneas de interrogación tanto en sus fundamentos como en sus extensiones posibles. Esta sección discute críticamente supuestos centrales del modelo, explora limitaciones de la aproximación adoptada, y sugiere direcciones para investigación futura.

El IVCE se construye sobre varios supuestos simplificadores que merecen escrutinio crítico. Primero, la modelización de costos como función determinística del ingreso puede no capturar heterogeneidades importantes entre individuos con niveles similares de ingreso pero diferentes dotaciones de capital humano, acceso a redes de soporte, o ubicación geográfica. En la realidad, dos individuos con ingreso y_i idéntico pueden enfrentar costos efectivos C_i^Q muy diferentes dependiendo de si residen en áreas urbanas con infraestructura digital desarrollada o en zonas rurales con conectividad limitada.

Segundo, el modelo asume que individuos pueden evaluar correctamente el valor de sus datos en riesgo V_i^D, lo cual requiere capacidades de procesamiento probabilístico y comprensión de amenazas futuras que pueden no estar distribuidas uniformemente en la población. Evidencia de estudios sobre brecha digital sugiere que poblaciones vulnerables frecuentemente tienen menor alfabetización digital, lo que podría implicar subvaloración sistemática de riesgos de seguridad de datos (Bulatova et al., 2023).

Tercero, el modelo trata la transición cripto-cuántica como un proceso dicotómico (adopción completa versus no adopción), cuando en realidad la adopción tecnológica frecuentemente ocurre de manera gradual y parcial. Individuos pueden adoptar protección cuántica para ciertos tipos de datos o transacciones mientras mantienen sistemas convencionales para otros usos. Esta adopción híbrida puede alterar tanto la estructura de costos como la efectividad de la protección de maneras no capturadas en la formulación actual.

Varias extensiones del modelo podrían enriquecer su capacidad explicativa y prescriptiva. Una primera extensión involucraría incorporar explícitamente dinámicas de aprendizaje y efectos de red. A medida que más individuos adoptan tecnologías cripto-cuánticas,

otros individuos pueden enfrentar costos de aprendizaje reducidos por disponibilidad de conocimiento acumulado en sus redes sociales. La literatura sobre difusión de innovaciones sugiere que estos efectos pueden ser particularmente importantes en contextos de tecnologías complejas que requieren alfabetización técnica especializada (López-Claros, 2011).

Una segunda extensión incorporaría heterogeneidad en preferencias de riesgo. Individuos con mayor aversión al riesgo deberían, ceteris paribus, valorar más altamente la protección de datos y estar dispuestos a destinar mayor fracción de ingreso a su adquisición. Esto sugiere modelar la capacidad de pago no solo como función del ingreso disponible sino también de parámetros de preferencia individual, donde individuos más aversos al riesgo tendrían disposición a pagar más alta para una misma configuración de ingreso y costos.

Una tercera extensión abordaría la dimensión internacional de la brecha cripto-cuántica. Países con diferentes niveles de desarrollo económico enfrentarán diferentes distribuciones del IVCE a nivel poblacional, y la conectividad global de sistemas digitales implica que vulnerabilidades en una jurisdicción pueden crear externalidades negativas para otras. Investigaciones sobre preparación societal para tecnologías cuánticas enfatizan necesidad de cooperación internacional y diplomacia cuántica para abordar estos desafíos globales (de Jong, 2022).

La naturaleza teórica del modelo presentado implica que su validación empírica enfrenta desafíos significativos, particularmente dada la fase temprana de despliegue comercial de tecnologías cripto-cuánticas. Sin embargo, ciertos componentes del modelo podrían calibrarse usando datos existentes sobre adopción de tecnologías de seguridad digital convencionales, diferencias de ingresos entre percentiles poblacionales, y estimaciones de valor económico de datos personales. La literatura emergente sobre impactos societales de tecnologías cuánticas sugiere que desarrollo de indicadores operacionalizables será crítico para informar políticas públicas efectivas (Vermaas, 2017).

La aplicabilidad del IVCE como instrumento de política requeriría desarrollo de metodologías de medición que respeten privacidad de poblaciones vulnerables cuya información se busca proteger, y mecanismos de actualización periódica del indicador a medida que evoluciona la tecnología cripto-cuántica y cambian distribuciones de ingreso. La traducción del marco teórico a recomendaciones de política específicas requeriría considerar contextos institucionales particulares, diferentes capacidades fiscales, estructuras regulatorias, y normas culturales sobre privacidad y protección de datos.

7. Conclusiones

Este artículo ha desarrollado un marco teórico para conceptualizar y medir la brecha de accesibilidad a tecnologías de criptografía cuántica entre diferentes segmentos socioeconómicos, con particular énfasis en poblaciones vulnerables. El Índice de Vulnerabilidad Cripto-Económica propuesto integra tres dimensiones fundamentales que interactúan de manera no lineal: los costos de transición tecnológica hacia sistemas de protección cuánticos, la capacidad económica de diferentes percentiles de ingreso para absorber dichos costos, y el valor económico de los datos personales en riesgo para cada segmento poblacional.

Los resultados teóricos principales pueden sintetizarse en tres proposiciones centrales. Primero, la estructura de costos de tecnologías cripto-cuánticas, caracterizada por componentes fijos elevados, genera una barrera de entrada absoluta que excluye a fracciones significativas de la población en economías con alta desigualdad de ingresos. Esta exclusión ocurre precisamente cuando la amenaza de sistemas criptográficos clásicos ante computación cuántica se vuelve más saliente, creando una ventana de vulnerabilidad elevada para poblaciones sin acceso a protección avanzada.

Segundo, la brecha de protección cripto-cuántica no constituye meramente una extensión de brechas digitales preexistentes, sino que presenta características distintivas que pueden amplificar desigualdades económicas de manera persistente. El valor económico de datos en riesgo para poblaciones vulnerables, aunque potencialmente menor en términos absolutos, representa frecuentemente una fracción mayor de su patrimonio total y tiene consecuencias proporcionalmente más severas sobre su bienestar. Esta asimetría entre necesidad de protección y capacidad de acceso genera una forma específica de injusticia distributiva en el contexto de transiciones tecnológicas, especialmente relevante dado que evidencia empírica documenta que grupos vulnerables ya enfrentan mayores riesgos durante procesos de automatización y transformación digital.

Tercero, la vulnerabilidad concentrada en segmentos poblacionales específicos genera externalidades negativas sistémicas que trascienden los costos privados de no protección. Sistemas digitales interconectados implican que la seguridad del conjunto depende críticamente de los eslabones más vulnerables, sugiriendo que la protección cripto-cuántica presenta características de bien público que justifican intervención colectiva más allá de decisiones individuales de adopción tecnológica.

Desde una perspectiva de política pública, el análisis sugiere que la transición hacia criptografía cuántica requiere atención explícita a dimensiones de equidad y accesibilidad económica. La ausencia de intervención podría resultar en una divergencia creciente entre poblaciones protegidas y vulnerables, con consecuencias negativas tanto en términos de bienestar de segmentos marginados como de estabilidad y seguridad del ecosistema digital

en su conjunto. Las opciones de intervención incluyen provisión pública de infraestructura cripto-cuántica como servicio básico, subsidios focalizados para segmentos de bajos ingresos, regulaciones de interoperabilidad que permitan transiciones graduales, y marcos redistributivos que reconozcan la protección de datos como componente de derechos digitales fundamentales.

El modelo desarrollado presenta limitaciones que sugieren direcciones para investigación futura. La incorporación de heterogeneidad en preferencias de riesgo, efectos de aprendizaje y redes sociales, y dimensiones internacionales de la brecha cripto-cuántica constituyen extensiones naturales que enriquecerían la capacidad explicativa del marco. Adicionalmente, el desarrollo de metodologías de validación empírica del IVCE una vez que datos sobre adopción de tecnologías cuánticas se vuelvan más disponibles constituye una agenda de investigación importante.

En términos más amplios, este trabajo contribuye a una literatura emergente que examina las implicaciones distributivas de tecnologías cuánticas. Mientras que gran parte de la discusión académica y política sobre computación cuántica se ha enfocado en dimensiones de competitividad geopolítica y ventajas estratégicas nacionales, las consecuencias para poblaciones vulnerables dentro de sociedades han recibido atención limitada. Investigaciones recientes demuestran que frameworks de equidad, diversidad e inclusión están completamente ausentes en la literatura técnica sobre tecnologías cuánticas, subrayando la urgencia de desarrollar marcos analíticos que expliciten dimensiones distributivas.

El análisis presentado sugiere que estas dimensiones de equidad no son secundarias sino centrales para evaluar la deseabilidad social de trayectorias de desarrollo tecnológico. El marco conceptual aquí desarrollado puede ser relevante más allá del contexto específico de criptografía cuántica, aplicándose a otras tecnologías emergentes que presentan estructuras similares de costos y distribución desigual de beneficios de protección entre segmentos socioeconómicos. En última instancia, la construcción de una era cuántica justa y equitativa requiere que consideraciones sobre accesibilidad y vulnerabilidad económica se integren desde las fases más tempranas del desarrollo tecnológico, evitando que brechas de protección se consoliden de manera irreversible.

Referencias

Bulatova, O., Reznikova, N., and Ivashchenko, O. (2023). Digital divide or digital inequality? new dimensions of global asymmetries of socio-economic development and international trade in the conditions of technoglobalism. *Vìsnik Marìupolskogo deržavnogo unìversitetu Serìâ Ekonomìka*, 13(25):45–57.

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.

Cukier, W. (2019). Disruptive processes and skills mismatches in the new economy. *Journal of Global Responsibility*, 10(3):211–225.

Dachs, B. (2017). The impact of new technologies on the labour market and the social economy.

Damayanti, C. (2024). Quantum ethics: Navigating the intersection of quantum mechanics and metaethics in the digital era for a just and equitable society. *Jurnal Filsafat*, 34(2):210.

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

Katz, R., Callorda, F., and Jung, J. (2021). The impact of automation on employment and its social implications: Evidence from chile. *Economics of Innovation and New Technology*, 32(5):646–662.

Kop, M. (2023). Quantum-elspi: A novel field of research. *Digital Society*, 2(2).

Krishnamurthy, V. (2022). Quantum technology and human rights: an agenda for collaboration. *Quantum Science and Technology*, 7(4):044003.

Kuban State Agrarian University, Volga State University, Moscow Technical University, and Samara State Economic University (2025). The impact of automation and artificial intelligence on social inequality. *Ekonomika i Upravlenie: Problemy, Resheniya*.

López-Claros, A. (2011). *The Innovation for Development Report 2010–2011*. Palgrave Macmillan UK.

Troyer, M., Benjamin, E. V., and Gevorkian, A. (2024). Quantum for good and the societal impact of quantum computing.

United Nations (2018). *World Economic and Social Survey 2018*. United Nations.

Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: a renewed urgency to make quantum theory understandable. *Ethics and Information Technology*, 19(4):241–246.

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.

Yolusever, A. (2025). Ai and automation: Reshaping the labor market. *Biga İktisadi ve İdari Bilimler Fakültesi Dergisi*, 6(1):63–85.

Young, S., Brooks, C., and Pridmore, J. (2024). Societal implications of quantum technologies through a technocriticism of quantum key distribution. *First Monday*.