# IMPACTOS DE LA COMPUTACIÓN CUÁNTICA EN LA SEGURIDAD DE SISTEMAS DE VOTACIÓN ELECTRÓNICA

COSTA, MATHEUS MOURA RODRIGUES; RIBEIRO, JOÃO VITOR FERNANDES; ROSÁRIO, PABLO ANDERSON AZEVEDO DO; SANTOS, MARIA EDUARDA NASCIMENTO DOS; SILVA, PAULO CAETANO DA

Universidade Salvador (UNIFACS)

matheusmoura.engcomp@gmail.com; joao.riba@hotmail.com; andersonpablo1007@gmail.com; m.eduardatech@hotmail.com; paulocaetano.dasilva@gmail.com

**RESUMEN**

La tecnología de computación cuántica, con su potencia de cálculo exponencialmente superior a la de las computadoras actuales, hace vulnerables los sistemas críticos, como los sistemas de votación electrónica, lo que significará un riesgo potencial para la integridad de la democracia. Este artículo analiza el impacto de la transición a un sistema de votación cuántica. Al examinar la literatura existente y simular protocolos en un entorno cuántico, el estudio evalúa los beneficios y desafíos relacionados con la seguridad, la integridad y la confiabilidad, con el objetivo de proteger los procesos democráticos contra futuras amenazas tecnológicas.

**PALABRAS CLAVES:** Computación cuántica; Seguridad; Voto electrónico; Protocolo cuántico.

**ABSTRACT**

Quantum computing technology, with its processing power exponentially superior to that of current computers, makes critical systems—such as electronic voting systems—vulnerable, that will mean a potential risk to the integrity of democracy. This article analyzes the impact of transitioning to a quantum voting system. By examining existing literature and simulating protocols in a quantum environment, the study evaluates the benefits and challenges related to security, integrity, and reliability, with the goal of protecting democratic processes against future technological threats.

**PALABRAS CLAVES:** Quantum computing; Security; E-Voting; Quantum Protocol.

## 1. INTRODUCCIÓN

La computación cuántica se ha convertido en una realidad con el potencial de desatar una importante revolución tecnológica en los próximos años. Trae consigo una potencia de cálculo increíblemente superior a la de los ordenadores tradicionales, lo que amenaza las medidas de seguridad y los algoritmos de cifrado actuales. En consecuencia, ha surgido la necesidad de iniciar un proceso de transición dentro de las grandes organizaciones (tanto públicas como privadas) hacia la adopción de sistemas cuánticos, con el objetivo de protegerse contra futuras amenazas y garantizar sistemas seguros y fiables.

Desde esta perspectiva, y considerando la inminente amenaza que el advenimiento de los ordenadores cuánticos representa para los protocolos criptográficos clásicos, los sistemas de voto electrónico se han convertido en el foco de atención de los investigadores. A lo largo de las últimas décadas, estos han propuesto protocolos cuánticos para garantizar la seguridad e integridad de dichos sistemas frente a ataques de ordenadores cuánticos.

Dado que los protocolos de voto cuántico existentes hasta ahora han demostrado ser ineficaces para garantizar simultáneamente la seguridad, la integridad y la verificabilidad (Arapinis et al., 2021), el proceso de transición a la computación cuántica, especialmente en los sistemas heredados (legacy), es sumamente complejo y costoso. Por lo tanto, es necesario comprender de qué manera este proceso podría resultar ventajoso en comparación con los métodos tradicionales y qué alternativas parecen más viables dentro del estado del arte actual en este campo.

Por todo esto, este trabajo busca resaltar los efectos de la computación cuántica en los sistemas de voto electrónico y responder a la siguiente pregunta: "¿Qué impacto puede tener el uso de la computación cuántica en los sistemas de voto electrónico y cómo mejora los niveles de seguridad en comparación con los sistemas tradicionales?". Así, el objetivo de este trabajo es investigar cómo se puede aplicar la computación cuántica dentro de un sistema de voto cuántico, analizando sus impactos en la seguridad, fiabilidad e integridad del sistema en un escenario de transición.

Este trabajo está organizado de modo que en la siguiente sección se repasan conceptos necesarios para la comprensión de este estudio, seguidamente se presenta la metodología de investigación, describiendo los pasos de la RSL (Revisión Sistemática de la Literatura) y la simulación de los protocolos en ambiente cuántico; en una tercera parte se presenta los resultados obtenidos a partir de la metodología aplicada; finalmente, se presenta la conclusión y las consideraciones finales correspondientes a los objetivos trazados.

## 2. MARCO TEÓRICO

Esta sección presenta los conceptos fundamentales que sustentan la realización y comprensión de este trabajo. En ella se abordan, respectivamente, las definiciones de computación cuántica, sistemas de voto electrónico y el sistema de votación brasileño.

### Computación cuántica

La computación cuántica se define como un campo emergente de la informática y la ingeniería que aprovecha las cualidades únicas de la mecánica cuántica para resolver problemas que escapan a la capacidad de los ordenadores más potentes (IBM, 2025).

El principal factor diferenciador de los ordenadores cuánticos en comparación con los ordenadores clásicos es que el procesamiento de datos se realiza mediante bits cuánticos, conocidos como cúbits (o qubits). Estos presentan propiedades concordantes con la base de los principios de la mecánica cuántica. Un cúbit puede presentar valores de 0 y 1, al igual que un bit clásico, pero también puede asumir ambos estados combinados simultáneamente.

Además, los cúbits tienen la capacidad de combinarse entre sí, lo que hace que la cadena de bits sea cada vez más compleja. El resultado es un sistema capaz de manipular la información con extrema rapidez, ejecutando operaciones que un ordenador clásico tardaría décadas en completar, ampliando así las posibilidades de crear nuevas aplicaciones.

**Sistemas de Votación Electrónica**

Los sistemas de voto electrónico actuales, basados en ordenadores clásicos, utilizan la seguridad criptográfica para la verificación de los votos y la prevención del fraude durante el proceso electoral. Sin embargo, con el avance y la difusión de herramientas con mayor potencia de cálculo, estos sistemas se han enfrentado a problemas y amenazas potenciales para garantizar la confianza y la integridad del voto. Entre estos problemas se encuentran la posibilidad de que un servidor central se vea comprometido mediante hackeo y se alteren los votos, la manipulación del software de las urnas electrónicas para desviar votos, la seguridad de los datos de votación transmitidos a través de internet y la falta de transparencia en el recuento de los votos.

Por lo tanto, la migración de los sistemas de votación hacia aquellos basados en la computación cuántica se vuelve esencial debido a las ventajas ofrecidas, derivadas de la aplicación de conceptos de la mecánica cuántica. Estos principios otorgan al sistema de voto cuántico la capacidad de ofrecer la máxima seguridad, a prueba de ordenadores clásicos e incluso de futuros ordenadores cuánticos, una detección precisa de actos fraudulentos, integridad garantizada y un anonimato robusto.

Sin embargo, a pesar de su gran potencial, todavía existen obstáculos para implementar un sistema de voto cuántico. Como la tecnología aún no ha alcanzado la madurez, mantener estados cuánticos estables sigue siendo muy difícil, lo que requiere equipos costosos y complejos con refrigeración a temperaturas cercanas al cero absoluto. Además, la falta de infraestructura, los altos costes y la complejidad que implica la auditoría de un sistema cuántico son otros problemas que todavía deben superarse para garantizar el funcionamiento estable de los sistemas de voto cuántico.

**El Sistema de Votación Electrónica en Brasil**

Los sistemas electorales brasileños se encuentran en una búsqueda de equilibrio entre la eficiencia administrativa y la garantía de la confiabilidad de la democracia. Por un lado, las innovaciones tecnológicas buscan la modernización, como el voto electrónico remoto (Albala et al. 2023), la aplicación de la tecnología *Blockchain*[5] (Fiori & Farina, 2022), o alteraciones de gobernanza en escenarios de sucesión extraordinaria (Barreto, 2022).

Por otro lado, los análisis críticos advierten sobre la no eliminación de vulnerabilidades estructurales que pueden introducir riesgos severos si no se fiscalizan correctamente (Marcacini & Barreto, 2019).

En resumen, la transición hacia modelos electrónicos complejos y descentralizados exige procesos graduales, inclusión digital y una gobernanza institucional transparente, capaz de salvaguardar el

[5] El blockchain es un tipo de libro-razón digital seguro, descentralizado y transparente que almacena datos en bloques conectados entre sí. Funciona sin necesidad de jefes o bancos, ya que miles de computadoras guardan una copia exacta de toda la información.

derecho a la privacidad y separar estrictamente la identidad del elector del voto computado. Sin embargo, el escenario de seguridad se vuelve aún más desafiante con la inminencia de la computación cuántica, un entorno tecnológico emergente y disruptivo que amenaza la criptografía convencional y pone en jaque la integridad de los sistemas vigentes. Esta realidad impone la necesidad urgente de estudios avanzados por parte de las autoridades electorales, justificando la investigación científica de nuevos protocolos de votación electrónica cuántica como salvaguarda para el futuro de la democracia.

## 3. METODOLOGÍA

Este trabajo es el resultado de los siguientes enfoques metodológicos: (i) una revisión sistemática de la literatura, utilizada para identificar el estado del arte, resumir las ideas de los trabajos más relevantes en el área y definir los criterios para evaluar los protocolos; (ii) la evaluación de los protocolos estudiados en el marco teórico, con un enfoque cuantitativo y cualitativo.

### Revisión Sistemática de la Literatura

Para asistir en el proceso de revisión sistemática de la literatura (Kitchenham & Charters, 2007), se utilizó la herramienta Parsifal[6], un gestor en línea y colaborativo que ayuda en la definición de las preguntas de investigación, la cadena de búsqueda (string de búsqueda) y la definición de los criterios de selección y calidad, además de la importación de artículos para la ejecución del tamizado.

Las preguntas de investigación, presentadas en la Tabla 1, buscaron discutir cómo la computación cuántica puede impactar diversas áreas y causar grandes cambios en los protocolos de seguridad futuros, en comparación con los modelos tradicionales utilizados actualmente.

***Tabla 1 - Preguntas de Investigación***

| Pregunta | Descripción |
|---|---|
| **RQ1** | ¿Cómo se utiliza la computación cuántica para mejorar los niveles de seguridad de los sistemas de votación? |
| **RQ2** | ¿Cuáles son las ventajas de la computación cuántica sobre la computación tradicional en los protocolos de seguridad de los sistemas de votación? |

***Fuente:*** *Elaboración propia (2026).*

Con base en las preguntas de investigación presentadas, y en la combinación de palabras clave referentes al artículo, se definió la cadena de búsqueda (string de búsqueda) utilizada para la búsqueda de la literatura sobre el tema en bibliotecas de gran prestigio en el universo de la tecnología de la información y de la computación, como la ACM Digital Library e IEEE Xplore.



[6] https://parsif.al/

Previamente, se realizaron pruebas de calidad de la cadena para evaluar su eficiencia en la localización de los artículos más relevantes.

| |
|---|
| *(“quantum computing” OR “quantum criptography” OR “quantum distribution keys”) AND (“security” OR “information security” OR “vote integrity” OR “voting system”)* |

Los criterios de inclusión y exclusión formaron parte de la selección inicial de artículos para la revisión, y se aplicaron de acuerdo con el enfoque principal del artículo, considerando la información presentada en el título, el resumen y las palabras clave. Los criterios de inclusión y exclusión utilizados se encuentran en la Tabla 2.

***Tabla 2 - Criterios de Inclusión y Exclusión***

| Criterios de Inclusión (I) | Criterios de Exclusión (E) |
|---|---|
| **I01:** ¿Este es un artículo de investigación? | **E01:** Artículo cuyo texto completo no puede ser accedido. |
| **I02:** ¿Hay una justificación para el motivo por el cual se realizó el estudio? | **E02:** Artículos publicados antes de 2020. |
| **I03:** ¿El artículo discute la utilización de la computación cuántica en los sistemas de votación? | **E03:** Artículos que no responden a las preguntas de investigación. |
| **I04:** ¿El artículo discute las ventajas de la computación cuántica sobre la computación tradicional en los sistemas de votación? | **E04:** Artículos que no sean de acceso abierto (*open access*). |
| **I05:** ¿El foco principal del estudio es el uso de la tecnología de la computación cuántica en la seguridad de los sistemas de votación? | |

***Fuente:*** *Elaboración propia (2026).*

Al finalizar la aplicación de los criterios de inclusión y exclusión, se seleccionó un total de 96 artículos: 30 de ellos pertenecientes a la biblioteca de ACM y 66 a la biblioteca de IEEE. Estos artículos fueron aprobados para la segunda selección inicial, correspondiente a los criterios de calidad.

Para evaluar los criterios de calidad, cada uno se definió con un peso máximo igual a 1.0 en caso de que el artículo cumpliera totalmente con el criterio. Si lo cumplía solo parcialmente, se aplicaba un peso de 0.5, y si no lo cumplía en absoluto, se aplicaba un peso de 0.0.

Los artículos considerados aptos luego de la aplicación de los criterios de calidad fueron aquellos que obtuvieron una puntuación mayor o igual al 75%.

- **Q01:** ¿El estudio reportó una investigación o fue solo un informe de "lecciones aprendidas" basado en la opinión de expertos?

- **Q02:** ¿Los objetivos y metas fueron reportados claramente (incluyendo una justificación del motivo por el cual se realizó el estudio)?
- **Q03:** ¿El diseño de la investigación fue apropiado para abordar los objetivos de la misma?
- **Q04:** ¿Hubo una descripción adecuada de los métodos utilizados para analizar los datos y estos métodos son apropiados para garantizar que el análisis esté fundamentado en dichos datos?
- **Q05:** ¿El estudio proporcionó hallazgos claramente declarados con resultados confiables y conclusiones justificadas?
- **Q06:** ¿Los resultados aportaron valor para la investigación o la práctica?

**Simulación de los Protocolos**

Através de la revisión sistemática de la literatura, se seleccionaron 4 protocolos de votación cuántica para ser validados en un entorno cuántico: Dual-Basis Measurement, Travelling Ballot, Distributed Ballot y Conjugate Coding.

Cada protocolo fue sometido a un escenario de votación predefinido que involucraba a 10 votantes, considerando un evento hipotético en el que se emitieron 8 votos como "Sí" y 2 votos como "No". Cada entorno de votación se simuló en función de su respectivo circuito cuántico, con un total de 500 ejecuciones (shots) por cada protocolo, para garantizar una mayor precisión en los resultados obtenidos de manera ágil. Finalmente, los resultados simulados se contabilizaron en base al escenario, calculando el número estimado de votos y la precisión de los resultados hallados en relación con los valores predefinidos.

Los protocolos fueron evaluados respecto de su grado de privacidad, confiabilidad y precisión en relación con los resultados obtenidos. De este modo, las discusiones se conducieron por un análisis comparativo, con el objetivo de comprender las ventajas de cada protocolo y cómo se pueden aprovechar y aplicar para crear protocolos más robustos y confiables que respalden un futuro sistema de votación electrónica cuántica.

## 4. RESULTADOS Y DISCUSIÓN

Esta sección presenta los resultados obtenidos de los análisis de los artículos seleccionados por la RSL y de la simulación y evaluación de los protocolos de votación cuántica, teniendo en cuenta los parámetros de privacidad, confiabilidad y precisión en el conteo de votos.

**Hallazgos de la RSL**

Tras la evaluación, se seleccionaron 10 artículos sobre la relación entre la computación cuántica y los sistemas de votación electrónica, enfocados principalmente en criptografía, ciberseguridad y comparaciones con blockchain. Estos trabajos permitieron identificar el estado del arte y los desafíos actuales de esta tecnología. A continuación, presentamos un breve resumen de los aspectos más relevantes de dichas investigaciones.

- **Gobernanza y Estructuración para la Transición Poscuántica:** La transición a la era poscuántica exige una fuerte preparación por parte de las organizaciones. Es fundamental adoptar modelos de gestión que mapeen las vulnerabilidades de seguridad (Khondokar et al., 2024) y refuercen la planificación estratégica para evitar el robo de datos en el presente con el objetivo de vulnerar su confidencialidad en el futuro (Mashatan & Heintzman, 2021). En el sector público, se nota una falta de directrices claras, lo que hace urgente que los gobiernos asuman un papel activo en la regulación y estandarización para evitar riesgos sistémicos en las infraestructuras digitales (Kong et al., 2024, 2022).
- **Desafíos Físicos y Tecnológicos en la Implementación Cuántica:** Aunque la tecnología cuántica ofrece un nivel de seguridad sin precedentes en teoría, su aplicación práctica aún se enfrenta a altos costos operativos y limitaciones físicas de la infraestructura de comunicación (Bajric, 2023; Nagpal et al., 2024). Para viabilizar la adopción corporativa, los investigadores se han enfocado en el desarrollo de alternativas tecnológicas más económicas que puedan adaptarse a las redes de comunicación que las empresas ya utilizan hoy en día (Barbosa, 2024).
- **Avances y Limitaciones en Sistemas de Votación Electrónica:** En el contexto de la toma de decisiones y procesos electorales, existen propuestas prometedoras para garantizar la privacidad absoluta de los votos utilizando conceptos cuánticos (Wu et al., 2021). Sin embargo, la literatura indica que las soluciones actuales aún presentan dificultades operativas para garantizar, de forma simultánea, la privacidad, la integridad de la información y la capacidad de auditoría (Arapinis et al., 2021). Para superar los cuellos de botella de procesamiento, la integración de tecnologías como Blockchain con modelos de seguridad optimizados ha demostrado ser un camino más viable (Geng et al., 2022).
- **Adopción de Enfoques Híbridos a Corto Plazo:** La literatura concuerda en que la protección inmediata de las organizaciones no exige la adopción de sistemas puramente cuánticos desde un principio. La recomendación gerencial a corto y mediano plazo es el uso de enfoques híbridos (Bajric, 2023; Mashatan & Heintzman, 2021). En la práctica, esto significa aliar los sistemas tradicionales ya existentes con nuevos modelos de defensa modernos, siempre con el apoyo de una gestión tecnológica estructurada (Arapinis et al., 2021; Geng et al., 2022; Khondokar et al., 2024). Esta estrategia garantiza una protección efectiva y viable mientras las nuevas tecnologías maduran.

**Resultados de la simulación de los protocolos**

A partir de la reproducción en un entorno cuántico de los cuatro protocolos estudiados a través de la RSL, se realizaron simulaciones para cada protocolo con el fin de evaluar los criterios seleccionados y llevar a cabo un análisis comparativo de las fortalezas y debilidades de cada uno. Posteriormente, se presentan los resultados obtenidos de estas simulaciones, considerando el escenario predefinido en la metodología.

Basándose en las simulaciones de los protocolos de votación cuántica descritos, una observación principal es su incapacidad para satisfacer plenamente los tres requisitos básicos de un sistema de votación. Aunque poseen características importantes para diversos escenarios — como la garantía de eficiencia en la mayoría de los casos —, se observó que solo un protocolo demostró garantizar la privacidad y el anonimato.

Además, aún no se ha comprobado que los protocolos de seguridad sean totalmente eficientes y, en algunas instancias, la complejidad y la exigencia de altos costos computacionales hacen que su aplicación resulte inviable. En la Figura 1 se presenta un resumen de los aspectos principales de cada protocolo.

***Figura 1 - Análisis Comparativo de los Protocolos***

| | Protocolo | Privacidad | Seguridad | Confiabilidad |
|---|---|---|---|---|
| 1 | Dual-Basis Measurement | Riesgo de acceso al voto individual. | Detección de fraude vía descarte de votos. | Resultado impreciso debido al descarte. |
| 2 | Travelling Ballot | Resultado agregado garantiza anonimato. | Vulnerable a colusión | Alta precisión en el conteo |
| 3 | Distributed Ballot | Risco de acceso ao voto individual. | Entrelazamiento cuántico garantiza integridad. | Precisión de 100%. |
| 4 | Conjugate Coding | Riesgo de acceso al voto individual. | Ineficiente/complejo debido al "cut-and-choose". | Precisión de 100%. |

***Fuente:*** *Elaboración propia (2026).*

A partir de este análisis, se evidencia la necesidad de un estudio continuo y profundo con el fin de identificar las fortalezas de cada protocolo y diseñar estrategias para aplicar estos atributos positivos a la creación de nuevos protocolos, más eficientes y que cumplan con los requisitos básicos establecidos en esta evaluación.

Por lo tanto, se concluye que el panorama de la computación cuántica para los sistemas de votación es altamente prometedor. Considerando la necesidad de estudios futuros para determinar métodos que permitan lograr protocolos cuánticos más robustos y confiables, los resultados obtenidos son de vital importancia para respaldar nuevas propuestas orientadas a un entorno cuántico más seguro para los sistemas de votación.

## 5. CONCLUSIÓN

A partir de la revisión de la literatura y los resultados, se concluye que los sistemas de votación cuántica son cada vez más robustos y aplicables, aunque sus protocolos aún carecen de eficiencia total. Aún deben superarse desafíos técnicos como la interferencia y la decoherencia cuántica, propiedades de la mecánica cuántica que generan márgenes de errores apreciables en el resultado de operaciones de cómputo. Estos factores ponen en riesgo la precisión y confiabilidad de los resultados en un escenario electoral.

Considerando esto, el objetivo planificado se alcanzó mediante simulaciones cuánticas que demostraron empíricamente las ventajas y desventajas de cada protocolo en cuanto a confiabilidad, integridad y privacidad. Esta validación práctica de la literatura resalta la necesidad de estudiar cómo aprovechar los mejores atributos de cada sistema para diseñar protocolos mucho más robustos y eficientes.

Para futuros trabajos, el principal desafío es profundizar en la mitigación de los problemas de interferencia y decoherencia. Los próximos estudios deben contemplar simulaciones a mayor escala, con un volumen superior de votantes y votos, así como la implementación directa en computadoras cuánticas reales para evaluar el rendimiento del sistema en entornos prácticos.

**6. REFERENCIAS**


Albala, A., Borges, A., & Rennó, L. (2023). Voto eletrônico remoto (i-voto) e a pandemia de COVID-19: uma proposta de política pública. *Revista de Sociologia E Política*, *31*. https://doi.org/10.1590/1678-98732331e014.

Arapinis, M., Lamprou, N., Kashefi, E., & Pappa, A. (2021). Definitions and Security of Quantum Electronic Voting. *ACM Transactions on Quantum Computing, 2(1), 1–33*. https://doi.org/10.1145/3450144.

Samed Bajrić. (2023). Enabling Secure and Trustworthy Quantum Networks: Current State-of-the-Art, Key Challenges, and Potential Solutions. *IEEE Access, 11, 128801–128809*. https://doi.org/10.1109/access.2023.3333020.

Barbosa, G. A. (2024). Digital Key Distribution Protected by Recorded Quantum Noise. *IEEE Access, 12*. https://doi.org/10.1109/access.2024.3462530.

Barreto, A. A. de B. (2022). Regulamentação da Eleição Presidencial Indireta no Ordenamento Jurídico Brasileiro: Impasses, Proposições e Desafios. *E-Legis - Revista Eletrônica Do Programa de Pós-Graduação Da Câmara Dos Deputados, 15(39), 1–23*. https://doi.org/10.51206/elegis.v15i39.763.

Geng, T., Laurent Njilla, & Huang, C. T. (2022). A Survey of Blockchain-Based Electronic Voting Mechanisms in Sensor Networks. https://doi.org/10.1145/3560905.3568181.

Khondokar Fida Hasan, Simpson, L., Rezazadeh, A., Islam, C., Rahman, Z., Armstrong, W., Praveen Gauravaram, & McKague, M. (2024). A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies. *IEEE Access, 12, 1–1*. https://doi.org/10.1109/access.2024.3360412.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. https://docs.edtechhub.org/lib/EDAG684W.

Kong, I., Janssen, M., & Bharosa, N. (2024). Deriving Government Roles for directing and supporting Quantum-safe Transitions. *Proceedings of the 25Th Annual International Conference on Digital Government Research, 507-514*. https://doi.org/10.1145/3657054.3657114.

Kong, I., Janssen, M., & Nitesh Bharosa. (2022). *Challenges in the Transition towards a Quantum-safe Government*. https://doi.org/10.1145/3543434.3543644.

Marcacini, A. T. R., & Barreto Junior, I. F. (2019). Aspectos jurídicos, políticos e técnicos sobre sistemas eletrônicos de votação e a urna eletrônica brasileira. *Revista Brasileira de Estudos Políticos*, *118*. https://doi.org/10.9732/rbep.v118i0.696.

Mashatan, A., & Heintzman, D. (2021). The Complex Path to Quantum Resistance. *Queue*, *19*(2), 65–92. https://doi.org/10.1145/3466132.3466779.

Nagpal, S., Gaba, S., Ishan Budhiraja, Sharma, M., Singh, A., Singh, K. K., Aksar, S. S., Abouhawwash, M., & Iwendi, C. (2024). Quantum Computing Integrated Patterns for Real-Time Cryptography in Assorted Domains. *IEEE Access*, *12*, 132317–132331. https://doi.org/10.1109/access.2024.3401162.

Schenider, J., Smalley, I. (2025). *Computação quântica*. IBM. https://www.ibm.com/br-pt/think/topics/quantum-computing.

Fiori Spagnol, L., & Farina, R. M. (2022). Um Sistema de Voto Eletrônico utilizando Blockchain. *RECIMA21 - Revista Científica Multidisciplinar - ISSN 2675-6218*, *3*(12), e3122421. https://doi.org/10.47820/recima21.v3i12.2421.

Wu, S., Sun, W., Wang, Q., Che, R., Hu, M., Ding, Z., & Xue, X. (2021). A Secure Quantum Protocol for Anonymous One-Vote Veto Voting. *IEEE Access*, *9*, 146841–146849. https://doi.org/10.1109/access.2021.3123681.