SCIENTIFIC REVIEW | REVIEW ARTICLE

Quantum computing, cybersecurity and financial sovereignty in Latin America

A rapid expert consultation

Emanuel Ortiz Ruiz[1,2], **Mario Góngora**[1,3] and **Eddie Velásquez**[1,4]

[1] Quantum Think Centre Colombia (QTC-CO), info@qtc-co.org

[2] Universidad EAN, Bogotá, Colombia, eeortiz@universidadean.edu.co

[3] De Montfort University, Leicester, United Kingdom, mgongora@dmu.ac.uk

[4] QuantPaths, United Kingdom, eddie@quantpaths.com

Correspondence: info@qtc-co.org |quantumthinkcentre.org| August 2026

Abstract

Context. Progress in quantum error correction, together with binding policy action in the United States and a coordinated roadmap in the European Union, is shortening the practical planning horizon for migration away from quantum-vulnerable public-key cryptography. Quantum computing now occupies, for cryptographic security, the position that artificial intelligence occupies for cybersecurity more broadly: a technology moving faster than the institutions that must absorb it.

Assessment. This rapid expert consultation examines the implications for Latin America, where exposure is amplified by long cryptographic replacement cycles, dependence on external standards and infrastructure, and uneven institutional capacity. The international consensus on both the threat and the response is now well formed, but it has been formed largely without Latin American authorship.

Argument. The relevant risk is not confined to a future cryptographically relevant quantum computer. Data captured today may be retained for later decryption, while an uneven global transition, reinforced by procurement and supervisory requirements in early-moving jurisdictions, could create operational and market-access disadvantages for institutions that cannot demonstrate quantum-safe controls.

Priorities. A regional response should combine shared cryptographic discovery, risk-based migration, crypto-agility, alignment with finalized standards, explicit supervisory timelines, continuous assurance, workforce development and scientific diplomacy. Colombia is presented as an illustrative case, not as a proxy for the entire region.

Keywords: quantum computing; post-quantum cryptography; crypto-agility; financial sovereignty; cyberdefence; Latin America; scientific diplomacy

Key points

- Quantum risk is governed by the interaction between data lifetime, migration time and the uncertain arrival of a cryptographically relevant quantum computer; the most consequential recent development is a shift in expectation, not a new machine.
- Harvest-now-decrypt-later collection makes long-lived information a present exposure, even before a large-scale fault-tolerant machine exists.
- The United States has set federal migration deadlines of 2030 and 2031 and is extending quantum-safe requirements to its contractors; the European Union is writing post-quantum planning into law. These external timelines will shape what Latin American institutions are asked to demonstrate.
- An uneven migration could translate technical unreadiness into higher counterparty risk, compliance costs or restricted access to international financial networks.
- The immediate priority is cryptographic discovery and dependency mapping, pursued as a regional common; followed by risk-based migration, measurable crypto-agility and supervisory timelines that convert recognition into obligation.
- Latin America needs sustained talent pipelines and a regional forum that can coordinate evidence, implementation and standards engagement, moving the region from rule-taker to co-author.

Introduction

Quantum computing has moved from a predominantly laboratory concern to a strategic planning issue for governments, financial institutions and operators of critical infrastructure. The central policy problem is not whether a precise date can be assigned to a cryptographically relevant quantum computer (CRQC), but whether institutions can complete complex cryptographic migrations before vulnerable information or services become exposed. This distinction is especially important in Latin America, where replacement cycles are long, specialist capacity is uneven and many critical digital services depend on global financial and technology infrastructures.

Rapid expert consultations are designed to synthesize the best available evidence and informed judgement when decision timelines are shorter than those of a full systematic review. The National Academies of Sciences, Engineering, and Medicine recently applied this model to the implications of artificial intelligence for cybersecurity, a field in which a general-purpose technology is outpacing the practices built to secure digital systems.[1] Quantum computing presents cryptographic security with a structurally similar problem, compressed into a narrower technical channel. Where artificial intelligence reshapes the whole attack surface, quantum computing threatens the specific mathematical assumptions on which public-key cryptography rests; but in both cases the pace of capability is outrunning the pace of institutional adaptation. We adapt the same decision-oriented logic to quantum computing, focusing on cybersecurity and financial sovereignty in Latin America and using Colombia as an illustrative national case.

The analysis has three objectives. First, it distinguishes technically grounded quantum risk from speculative timelines. Second, it examines how policy asymmetries between early-moving

jurisdictions and the region could affect Latin American financial and security institutions. Third, it proposes a practical regional agenda organized around the six QTC-CO pillars: science with purpose, technology with conscience, diplomacy with impact, sovereignty and cyberdefence, sustainability, and inclusion and equity.

The risk horizon is contracting

A shift in expectation rather than a new machine

The most consequential development of the past year is not a new machine but a change in what experts expect one to require. Gidney estimated that factoring an RSA-2048 integer could be feasible in less than one week using fewer than one million noisy qubits, under explicit assumptions about error rates, connectivity, cycle times and control latency.[2] The comparable estimate published six years earlier by Gidney and Ekerå had been roughly 20 million noisy qubits, so the resource requirement has fallen by more than an order of magnitude without any corresponding leap in deployed hardware.[3] This is not evidence that such a machine exists, nor is it a forecast of its delivery date. It is evidence that algorithmic and error-correction improvements can materially reduce estimated attack resources, and that planning assumptions anchored to older estimates may already be stale.

Planning under uncertainty: the Mosca inequality

The Mosca inequality provides a more defensible planning framework than any single Q-Day prediction. If the required confidentiality lifetime of data plus the time needed to migrate the systems that protect it exceeds the time until a capable adversary obtains a CRQC, the institution is already outside a safe planning window.[4] The variables are uncertain, but uncertainty does not eliminate the exposure. It requires scenario analysis, explicit confidence ranges and earlier action for information with long confidentiality horizons. For institutions holding financial records, health data or state secrets, whose confidentiality must persist for a decade or more, the inequality is in many plausible scenarios already unfavourable.

Harvest-now-decrypt-later operations further shift the risk into the present. Encrypted traffic, archives and credentials collected today may retain intelligence or commercial value when cryptanalytic capability improves. Consequently, prioritization should begin with information whose sensitivity persists for years — state secrets, identity data, health records, intellectual property and high-value financial information — rather than with whichever application is easiest to migrate. Taken together, the falling resource estimates and the ongoing collection of long-lived data collapse the runway available for what is inherently a multi-year migration.

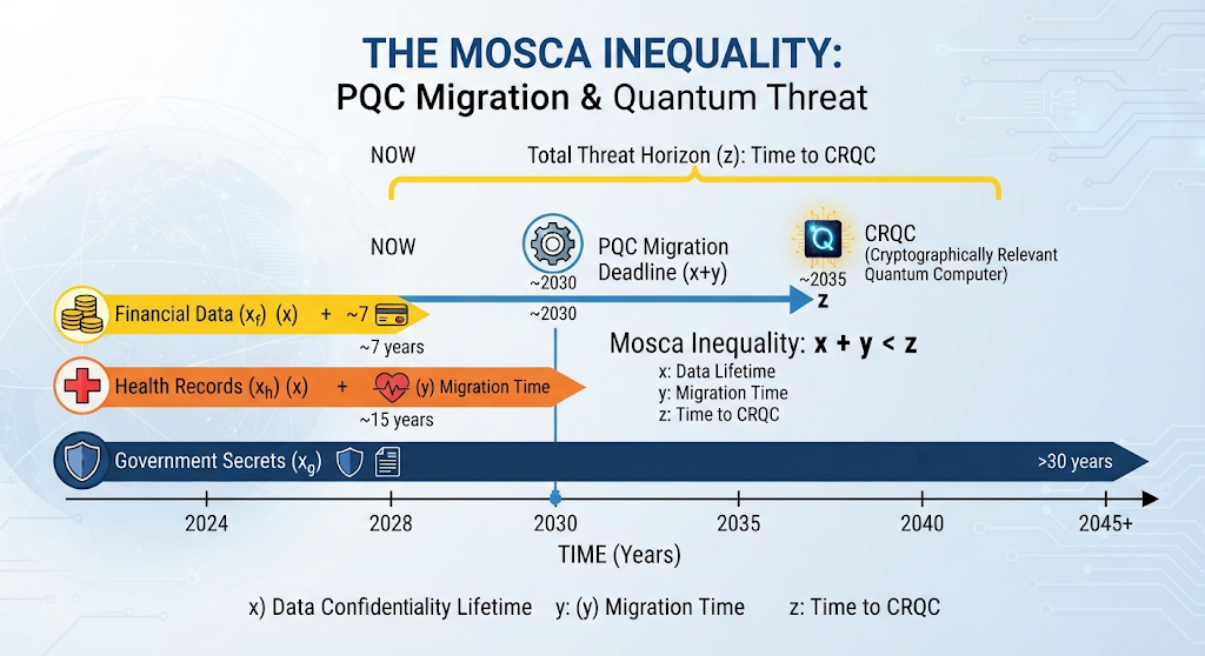

Figure 1

Major powers are treating quantum capability as infrastructure

The United States

On 22 June 2026 the United States issued two complementary executive orders. Executive Order 14413, *Ushering in the Next Frontier of Quantum Innovation*, calls for a whole-of-government quantum strategy spanning computing, sensing, networking, workforce, supply chains, security and international engagement.[5] It establishes the Quantum Computer for Application Development and Discovery Science effort at a Department of Energy facility, directs the development of national benchmarking capacity and requires assessment of the national-security implications of increasingly capable commercial quantum systems, including implications for post-quantum migration.

Its companion order, *Securing the Nation Against Advanced Cryptographic Attacks*, supplies the deadlines.[6] Federal high-value assets and high-impact systems must complete migration to post-quantum key establishment by the end of 2030 and to post-quantum digital signatures by the end of 2031, with a pilot to be completed by 2027. This pulls the previous government-wide target of 2035, set in 2022, forward by four to five years.[7] Notably for other jurisdictions, the order also directs federal procurement rules to require covered contractors to comply with the finalized NIST standards by the end of 2030. Quantum-safe cryptography is thereby becoming a condition of doing business with the United States government, and by extension with the many private counterparties that align their own requirements to federal expectations.

Separately, the proposed National Quantum Initiative Reauthorization Act of 2026 would extend federal programmes through 2034 and add the security of quantum supply chains, workforce retention and cooperative research with allies as explicit statutory purposes.[8] Together, these instruments frame quantum technology as economic and national-security infrastructure — infrastructure of state — although the proposed legislation should not be treated as enacted law unless and until the legislative process is complete.

The European Union

The European Union has paired strategic ambition with a coordinated post-quantum implementation roadmap. The roadmap calls on Member States to begin transition activities by the end of 2026, to protect critical infrastructure by the end of 2030 and to complete broader migration by 2035.[9] These dates are recommendations rather than binding obligations, and implementation will still depend on sectoral guidance, procurement cycles, certification capacity and coordination across national jurisdictions. The regulatory machinery is, however, becoming more explicit. In January 2026 the Commission proposed a targeted amendment to the NIS2 Directive that would require every Member State to adopt, within its national cybersecurity strategy, dedicated policies for the transition to post-quantum cryptography aligned with those timelines.[10] If adopted, post-quantum planning would move from an interpretive expectation to a named statutory component of national strategy, and an anticipated Quantum Act is intended to institutionalize and fund the broader strategy.

Europe's experience also carries a cautionary lesson that is directly relevant to Latin America. Despite a scientific base that the Commission itself describes as world-leading, Europe attracts only about 5% of global private quantum funding, against more than 50% captured by the United States, with the gap most pronounced at the later stages of company growth.[11] Strategy, roadmaps and public research funding do not, by themselves, secure sovereignty. Without sustained investment and a route to commercialization, a strong science base can become a source of talent and intellectual property for better-capitalized ecosystems elsewhere. A region whose scientific output already exceeds its capital base should take note.

Multilateral finance

Multilateral financial institutions have treated quantum computing as a financial-stability and operational-resilience issue for several years. International Monetary Fund analyses have recommended inventories of public-key cryptography, migration to quantum-resistant algorithms and cryptographic agility, and have positioned the Fund as an advocate of quantum-safe standards among its members.[12,13] The World Economic Forum has likewise urged financial-services leaders to integrate quantum readiness into strategy and risk governance.[14] A broad policy direction is therefore emerging among governments, standards bodies and financial institutions, even though the timing, scope and assurance requirements of migration remain heterogeneous. That consensus is being formed, however, largely without Latin American authorship.

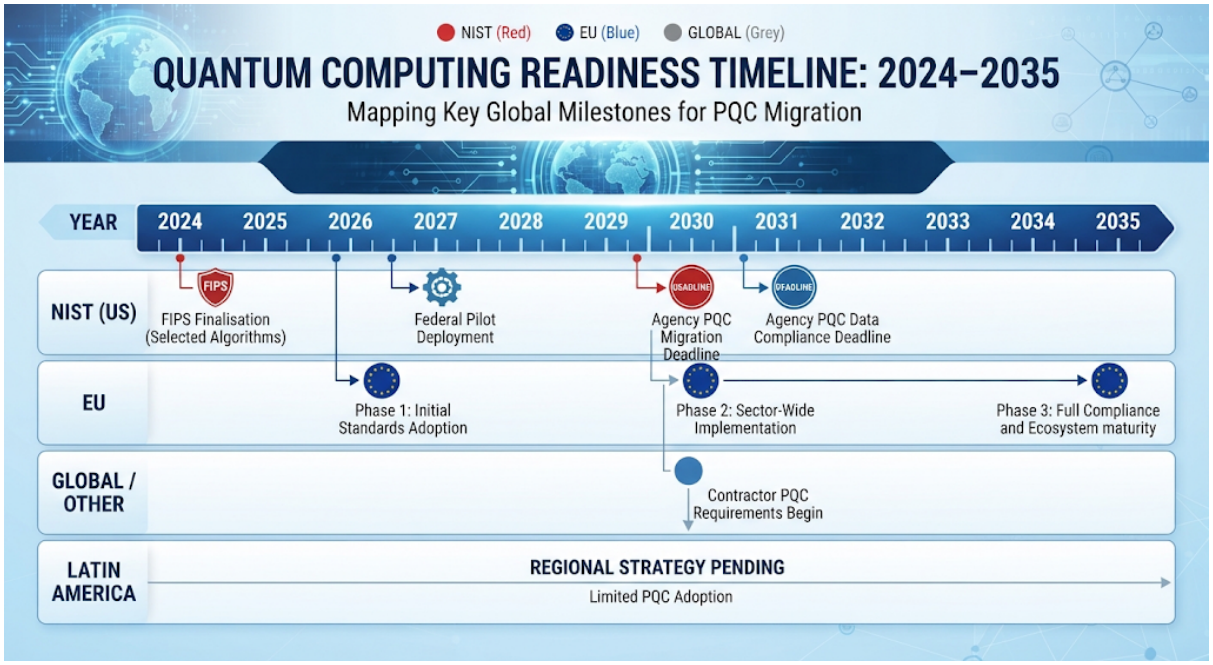

Figure 2

Method and scope

This article is a rapid, narrative expert consultation rather than a systematic review. The format is appropriate to a fast-moving field in which the policy-relevant question — what should Latin America do now? — is more urgent than any single unresolved empirical dispute. It integrates three source classes: primary policy and legal instruments; technical literature on quantum attack resources and cryptographic migration; and institutional or regional assessments of financial-sector exposure, skills and readiness. Evidence was interpreted through the QTC-CO six-pillar framework to connect technical risk with governance, sovereignty and equity.

Three limitations qualify the conclusions. First, CRQC timelines remain deeply uncertain, and resource estimates depend on hardware and architectural assumptions; the article therefore treats them as planning parameters rather than predictions. Second, comparable regional readiness data are sparse; several Latin American indicators originate in industry reporting rather than peer-reviewed surveys. Third, the consultation is selective and decision-oriented. It identifies robust actions under uncertainty but does not estimate the probability or exact timing of Q-Day. Numerical claims from secondary sources should therefore be independently validated before they are used for regulatory baselines or investment decisions.

Implications for Latin America

Cryptographic migration is a sovereignty issue

Post-quantum migration is not a routine software upgrade. Public-key cryptography is embedded in identity systems, payment rails, digital signatures, virtual private networks, hardware security modules, certificates, code-signing processes, connected devices and supplier services. The transition therefore crosses institutional boundaries and exposes dependencies that no single technology team controls. And because whoever authors and certifies the underlying standards effectively shapes the

security posture of everyone who adopts them, a region that adopts standards it did not help design, on timelines it did not help set, becomes a rule-taker in one of the defining infrastructures of the coming decade.

For Latin America, however, sovereignty should not be equated with developing isolated regional cryptographic algorithms. A more credible objective is informed participation: the capacity to evaluate standards, influence implementation profiles, build local assurance and testing capability, negotiate procurement requirements and retain the ability to change algorithms without unacceptable disruption. Sovereignty in this sense is operational agency within an interoperable global system — the difference between inheriting priorities and having them represented.

Uneven migration could amplify financial exclusion

An asymmetric transition could divide financial institutions into those able to demonstrate quantum-safe controls and those unable to do so. The World Economic Forum has described the prospect of a two-tier global financial system arising from unequal access to quantum-safe capabilities.[15] The likely mechanism is not instantaneous disconnection on Q-Day; it is a gradual repricing of operational and counterparty risk through due diligence, insurance, correspondent-banking requirements, procurement standards and supervisory expectations. The United States contractor requirement described above is an early instance of that mechanism at work: once quantum-safe cryptography becomes a condition of supplying one major government, it tends to propagate through the supply chains and counterparty relationships that connect to it.

Latin American institutions that depend on counterparties in jurisdictions with earlier migration deadlines could therefore face duplicated compliance costs or constrained market access. Colombia illustrates the governance gap: reporting cited in the regional literature points to a high and rising volume of attempted cyberattacks against the financial system, and the national financial supervisor has identified quantum computing as a coming priority, while formal quantum-specific migration requirements, deadlines and guidance remain limited.[16] These reports signal urgency but should not substitute for regulator-validated incident metrics. The more defensible conclusion is that awareness has not yet matured into a sequenced, measurable migration programme.

Equity is part of the security problem

The distributional consequences of the transition are significant. Countries that already concentrate capital, laboratories, advanced manufacturing and standard-setting influence are also best positioned to absorb migration costs. Without coordinated financing, open training resources and shared assurance infrastructure, post-quantum requirements could widen technological and financial asymmetries between the Global North and the Global South.

Equity is therefore not an adjacent social objective; it is a condition of collective security. Weak migration capacity in one part of an interconnected payment, communications or supply-chain network can create exposure elsewhere. Regional cooperation can reduce this asymmetry by pooling scarce expertise, reference architectures, test environments and procurement knowledge. For a regional actor such as QTC-CO, equitable access to quantum knowledge and quantum-safe infrastructure is thus both a value commitment and a strategic imperative.

Talent is a binding constraint

For most Latin American institutions, near-term readiness depends less on direct access to quantum hardware than on people able to discover cryptographic dependencies, interpret standards, redesign protocols, validate implementations and govern multi-year programmes. A 2026 regional business survey found that roughly seven in ten Latin American organizations identified a shortage of quantum expertise as an obstacle to adopting the technology, and concluded that institutional preparedness matters as much as the maturity of the hardware itself.[17] Because the underlying sampling and methodology require scrutiny, the figure is best treated as an indicative signal rather than a population estimate.

The policy implication is nevertheless robust: education strategy and cyber-resilience strategy are inseparable. Colombia's ColombIA Inteligente 2025 call, which included support for artificial intelligence and quantum research, indicates public interest that could be translated into durable capability through sustained funding, common competence frameworks and institutional partnerships.[18] Short courses alone will not suffice. The region needs pathways from foundational science to cryptographic engineering, audit, policy and executive risk ownership: quantum and post-quantum content embedded across university curricula rather than confined to specialized electives; apprenticeship and rotational placements in which junior practitioners build foundational reasoning while working on real migration problems; and international double-degree and exchange arrangements of the kind QTC-CO is developing with partner universities.

A regional action agenda

The following actions mirror the structure of the National Academies consultation while extending it with two elements that reflect the mandate of a regional convening institution: explicit supervisory timelines and scientific diplomacy.[1] They are offered as options for decision-makers rather than as prescriptions, and they are sequenced so that each creates the evidence base the next requires.

1 Discover the cryptographic estate — as a regional commons

Create institution-wide inventories of cryptographic assets and dependencies, including certificates, protocols, key-management systems, code-signing, embedded devices, cloud services and third-party products. Record algorithm, key size, purpose, owner, data lifetime, replacement path and supplier constraints. Discovery should be repeatable and integrated into asset and configuration management. Just as the National Academies called for shared evaluation infrastructure for AI-enabled cyber capabilities, the region needs shared capacity to measure its own exposure: a coordinated effort that pools discovery methods, tooling and expertise across academia, government and industry would allow smaller institutions to inventory and prioritize far faster than each could alone, and would establish crypto-agility as a regional baseline rather than a privilege of the largest institutions.

2 Prioritize by consequence and confidentiality horizon

Rank migrations using service criticality, exposure, data lifetime, interoperability and feasibility. Systems protecting long-lived secrets or safety-critical operations should precede low-consequence systems, even when the latter are easier to replace. Use multiple CRQC scenarios rather than a single forecast.

3 Align with finalized standards and preserve agility

Adopt standardized algorithms and implementation profiles as they mature, rather than waiting for regional variants. NIST has finalized ML-KEM, ML-DSA and SLH-DSA in FIPS 203, FIPS 204 and FIPS 205, respectively.[19–21] Migration designs should support algorithm substitution, version negotiation, key rotation, rollback and hybrid operation where required by risk, interoperability or policy. Hybrid designs should be treated as engineered transition mechanisms, not as permanent substitutes for governance.

4 Use the transition window deliberately: supervisory timelines

The window opened by the gap between planning and a functioning CRQC is finite and should be used, not merely observed. Institutions cannot close that window on their own; the actions above are far more likely to be resourced where regulators have converted stated recognition of quantum risk into explicit expectations. National financial supervisors, telecommunications regulators and cybersecurity authorities should therefore publish sector-specific migration timelines, inventory and reporting requirements and assurance expectations, analogous in structure to those now set in the United States and the European Union but calibrated to regional replacement cycles and capacity. Supervisory deadlines would give mid-sized institutions the clarity they currently lack, allow boards to justify multi-year budgets and create a defensible domestic baseline against which foreign counterparty requirements can be negotiated rather than simply absorbed.

5 Establish continuous assurance

Treat quantum readiness as an operating posture rather than a one-off project. Inventory, migration, testing, monitoring, incident response and supplier assurance should update one another continuously, so that new systems are quantum-safe by default and legacy exposure is retired progressively rather than in a single, disruptive effort. Metrics should track cryptographic coverage, unknown dependencies, migration lead time, exception age, test results and residual exposure.

6 Build the workforce and implementation commons

Develop shared curricula and role-based competence frameworks spanning science, engineering, audit, law, procurement and executive governance, so that training is comparable and portable across the region. Regional laboratories, apprenticeships, faculty exchanges and double-degree arrangements can distribute scarce expertise more efficiently than isolated national initiatives, and can spread the cost of scarce instructors and laboratory resources across many more learners than any single institution could reach.

7 Use scientific diplomacy to coordinate the transition

Create a regional convening node able to connect academia, government, defence, financial institutions, telecommunications operators and technology suppliers. Its purpose should be to share evidence, develop interoperable implementation profiles, represent regional constraints in international forums and publish transparent readiness measures. Scientific diplomacy converts fragmented national efforts into a shared regional voice, which is the only realistic path from rule-taker to co-author of the standards the region will live with.

Box 1 | Minimum evidence for a credible quantum-readiness programme

Scope. Named business services, systems, suppliers and information classes; explicit treatment of operational technology and embedded devices where relevant.

Baseline. A reproducible cryptographic inventory with ownership, algorithm use, data lifetime and dependency mapping.

Prioritization. Documented risk criteria and scenario assumptions, including migration duration and confidentiality horizon.

Architecture. Approved target profiles for key establishment, signatures, certificates, key management, hybrid operation and rollback.

Assurance. Interoperability, performance, failure-mode and security testing, with evidence retained for audit.

Governance. Executive accountability, funded milestones, supplier obligations, exception management and measurable residual risk.

Supervision. Alignment with any published national timeline, and a documented position on the foreign counterparty and procurement requirements the institution expects to meet.

The role of QTC-CO

QTC-CO can contribute most credibly as an evidence and coordination institution that articulates academia, national defence, industry and international diplomacy around an ethical and sovereign quantum agenda. Its six-pillar framework provides a useful bridge between technical migration and the wider objectives of ethical deployment, sustainability, national resilience and regional inclusion. The centre should avoid presenting uncertainty as certainty; its comparative advantage is to translate uncertainty into transparent scenarios, testable requirements and coordinated action.

A practical mandate would include a regional cryptographic-inventory methodology, reference implementation profiles, independent readiness assessments, training pathways and a forum for scientific diplomacy. A quantum-governance index could support accountability if its indicators, weights, data sources and limitations are published and independently reviewable. The value of such an index would lie in reproducibility and institutional learning, not in a single composite score.

Conclusion

Quantum computing creates an unusual policy problem: the date of decisive cryptanalytic capability is uncertain, but the time required to replace vulnerable cryptography is long and the confidentiality clock for captured data is already running. Waiting for certainty therefore transfers risk to institutions with the least time and capacity to respond — and, as the deadlines now set in Washington and Brussels make clear, the terms of the transition are being written whether or not the region takes part in writing them.

Latin America can reduce that exposure without attempting to predict Q-Day or reproduce the full industrial strategies of larger economies. The immediate agenda is concrete: discover cryptographic dependencies as a shared regional effort, prioritize long-lived and critical assets, migrate toward

finalized standards, engineer crypto-agility, give institutions supervisory timelines they can plan against, test continuously, develop specialist talent and coordinate regionally. Pursued together, these measures turn quantum readiness from a narrative of technological dependence into a programme of operational agency and financial resilience — and move the region from rule-taker to co-author.

Author contributions and declarations

Emanuel Ortiz Ruiz leads the National Defence line, Mario Góngora serves as Scientific Lead, and Eddie Velásquez leads the Industry and Telecommunications line at QTC-CO. All authors contributed to the conceptual framing, expert interpretation and manuscript development. The authors declare no competing interests. This article is an institutional analytical brief and has not been presented as a systematic review or consensus statement.

References

1. National Academies of Sciences, Engineering, and Medicine. Implications of recent advancements in artificial intelligence for cybersecurity: a rapid expert consultation. National Academies Press (2026). https://nap.nationalacademies.org/resource/29493/interactive

2. Gidney, C. How to factor 2048-bit RSA integers with less than a million noisy qubits. arXiv:2505.15917 (2025). https://doi.org/10.48550/arXiv.2505.15917

3. Gidney, C. & Ekerå, M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum 5, 433 (2021). https://doi.org/10.22331/q-2021-04-15-433

4. Mosca, M. Cybersecurity in an era with quantum computers: will we be ready? IEEE Security & Privacy 16, 38–41 (2018). https://doi.org/10.1109/MSP.2018.3761723

5. The White House. Executive Order 14413: Ushering in the Next Frontier of Quantum Innovation (22 June 2026). https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-next-frontier-of-quantum-innovation/

6. The White House. Executive Order: Securing the Nation Against Advanced Cryptographic Attacks (22 June 2026). [Verify executive order number and URL against the Federal Register before submission.]

7. The White House. National Security Memorandum 10: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (4 May 2022).

8. National Quantum Initiative Reauthorization Act of 2026, S. 3597, 119th Congress (2026). https://www.congress.gov/bill/119th-congress/senate-bill/3597

9. European Commission. A coordinated implementation roadmap for the transition to post-quantum cryptography (2025). https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

10. European Commission. Proposal for a Directive amending Directive (EU) 2022/2555 (NIS2). COM(2026) 13 final (20 January 2026).

11. European Commission. Quantum Europe Strategy: Quantum Europe in a changing world. COM(2025) 363 final (2 July 2025). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0363

12. Deodoro, J., Gorbanyov, M., Malaika, M. & Saadi Sedik, T. Quantum computing's possibilities and perils. Finance & Development 58(3) (2021). https://www.imf.org/en/publications/fandd/issues/2021/09/quantum-computings-possibilitiesand-perils-deodoro

13. Deodoro, J., Gorbanyov, M., Malaika, M. & Saadi Sedik, T. Quantum computing and the financial system: spooky action at a distance? IMF Working Paper 2021/071 (2021).

14. World Economic Forum. Quantum technologies: key strategies and opportunities for financial services leaders (2025). https://reports.weforum.org/docs/WEF_Quantum_Technologies_Key_Strategies_and_Opportunities_for_Financial_Services_Leaders_2025.pdf

15. World Economic Forum. How quantum computing can prevent a two-tier global financial system (30 January 2026). https://www.weforum.org/stories/2026/01/quantum-divide-two-tier-global-financial-system/

16. Cyte. The global financial system already has a quantum-safe strategy to combat cyberattacks. Latin America has yet to develop its own (2026). https://www.cyte.co/en/post/financial-system-quantumsafe-plan-cyberattacks-latin-america

17. Mexico Business News. Quantum computing is closer than we think. Are we ready? (7 May 2026). https://mexicobusiness.news/tech/news/quantum-computing-closer-we-think-are-we-ready

18. Ministerio de Ciencia, Tecnología e Innovación. ColombIA Inteligente 2025 [funding call] (Government of Colombia, 2025).

19. National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard. FIPS 203 (2024). https://doi.org/10.6028/NIST.FIPS.203

20. National Institute of Standards and Technology. Module-lattice-based digital signature standard. FIPS 204 (2024). https://doi.org/10.6028/NIST.FIPS.204

21. National Institute of Standards and Technology. Stateless hash-based digital signature standard. FIPS 205 (2024). https://doi.org/10.6028/NIST.FIPS.205