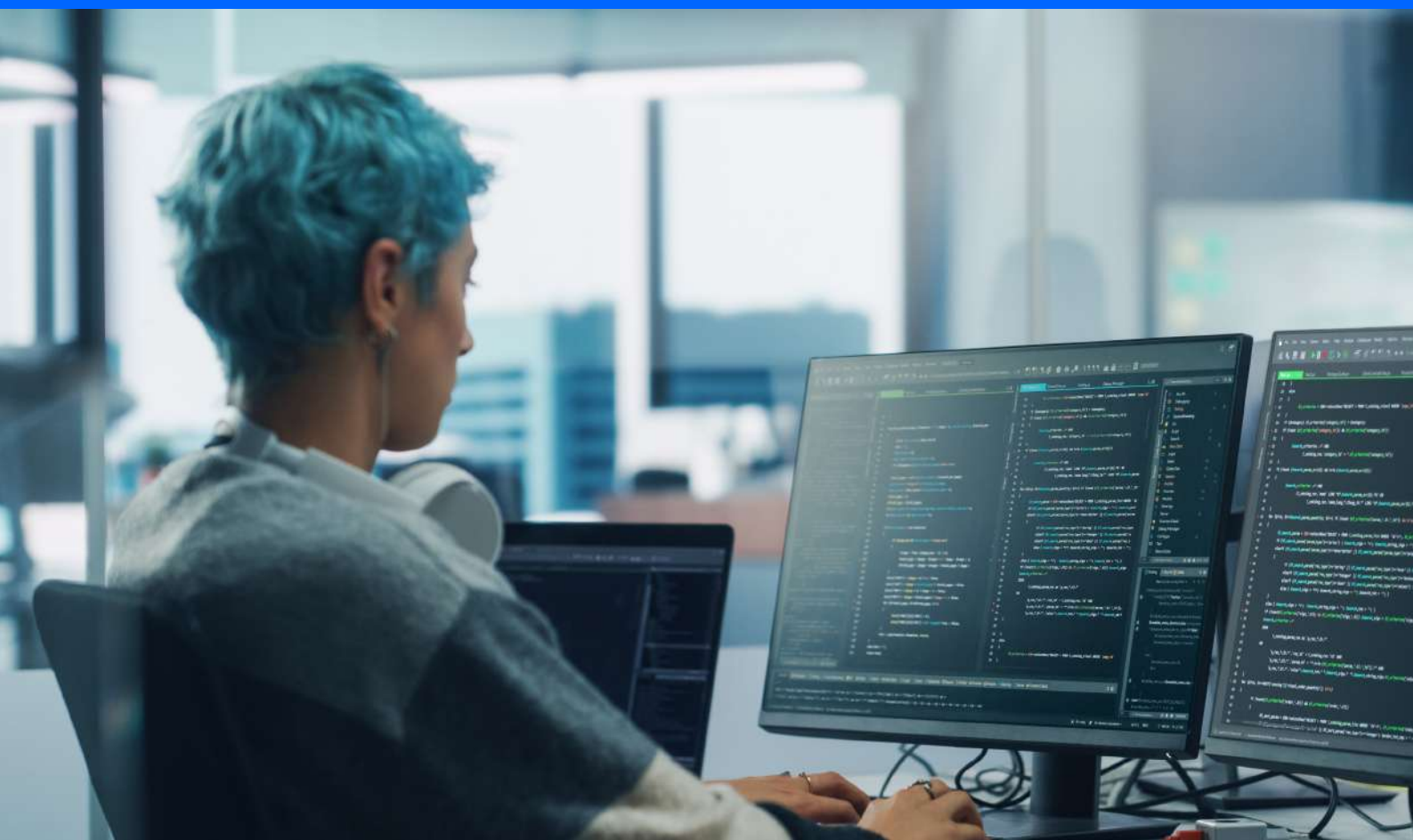
Telefónica Tech

Strategic preparation for Post-Quantum Cryptography

The threat of quantum computing, the implementation of post-quantum cryptography (PQC), and strategies for a secure and effective transition.



Index

Summary

Cryptography is essential for digital security and sovereignty. However, the current asymmetric cryptographic systems will be vulnerable with quantum computing. This calls for a transition to post-quantum cryptography (PQC).

This paper outlines the risks, transition strategies, and recommended actions to protect information in the quantum era.

Introduction

Digital sovereignty is key to ensuring the independence and control of infrastructures and data. This principle encompasses operational, technological and data management dimensions, and forms the basis for the autonomy of organizations and states.

Cryptography is the technological basis of sovereignty that provides this control and autonomy. It ensures the confidentiality, integrity, and availability of data, fundamental to the functioning of companies, governments, and societies.

However, this security paradigm faces a significant change with the advance of quantum computing. The Q-Day moment, when quantum computers can compromise current systems, could come in 10 to 20 years, if not sooner. Although there is no exact consensus, and this projection depends on progress in quantum computing and the scalability of qubits, this requires preparation to ensure the security of data and communication networks.

Post-quantum cryptography (PQC) emerges as a technical response. It develops encryption algorithms resistant to attacks by classical and quantum computers, based on mathematical problems that quantum computers cannot solve efficiently. This provides a level of security adapted to the quantum era.

The adoption of post-quantum cryptography is beyond the purely technical. It is a strategic decision with implications for the sovereignty of digital infrastructures. Organizations, companies, and governments ensure that their data and infrastructures are protected against present and future threats by implementing PQC. In doing so, they reaffirm their ability to operate independently, maintaining control over their digital assets and preserving their sovereignty.

What would be the consequences if someone intercepted and stored your company's most sensitive data and decrypted it in 2030?

This document lays out a call to action for organizations, companies, and national agencies. It is urgent to prepare for the transition to PQC now. Delaying this action could have significant consequences, including exposure of sensitive data, disruption of operations, and regulatory non-compliance.

Post-quantum cryptography **is deployable on conventional hardware and software.** This makes it possible to start the transition today to ensure the resilience and reliability of the digital infrastructure in the future.

The role of cryptography in data protection and digital sovereignty in the post-quantum era

Encryption protects data from unauthorized access and ensures digital sovereignty in storage, communications, and cloud. It prevents surveillance or external interference, safeguarding communications from governments, organizations or malicious actors.

Regulations such as RGPD in Europe require encryption to ensure user privacy and personal data protection. In addition, encryption protects critical infrastructures such as telecommunications, energy and financial services, safeguarding operational data and control systems.

It is crucial to prepare now and migrate to new quantum cryptographic algorithms to preserve data protection and digital sovereignty in the long term.

Impact on current cryptography

The most significant potential impact of quantum computing from a cyber security point of view is its ability to compromise the security of many asymmetric (public key) cryptographic algorithms used today.

- **Algorithms at risk:** RSA, DSA, ECDSA and others based on the difficulty of large integer factoring or the discrete logarithm problem are vulnerable to attack by a cryptographically relevant quantum computer. These algorithms are the basis for the security of protocols such as TLS / SSL (used in HTTPS), SSH, digital signatures and many public key infrastructures (PKI).
- **Symmetric cryptography (AES, SHA-256):** Although quantum computing affects symmetric cryptography through algorithms such as Grover's, the impact is less severe. An increase in key size would be required to maintain an equivalent level of security. For example, AES-256 offers 128 bits of security against quantum attacks (according to Grover's algorithm), which is equivalent to the classical security of AES-128. In quantum attacks, AES requires an increase in key length to maintain its security level.

The threat of the 'Harvest now, decrypt later' strategy

Malicious actors have adopted the Harvest Now, Decrypt Later (HNDL), or 'Store Now, Decrypt Later', attack strategy as a long-term tactic.

HNDL involves the mass collection of encrypted data using traditional techniques for storage and decryption with cryptographically relevant quantum computers. This affects information with a long period of confidentiality, such as government secrets, intellectual property or medical records, among others.

HNDL attacks of massive collection of encrypted data from APT (Advanced Persistent Threat) groups linked to nation-states have been identified, including interception of communications exploiting vulnerabilities in VPN networks or TLS channels, exfiltration of cloud storages with encrypted information, or traffic redirection.

Key quantum algorithms: Shor and Grover

- **Shor's algorithm:** This algorithm, developed by Peter Shor, is the main threat to current asymmetric cryptography. It allows factoring large integers in polynomial time, a significant advance over the best classical algorithms. This invalidates the security of RSA and similar algorithms and means that data encrypted today with these schemes could be decrypted in the future.

- **Grover's algorithm:** Lov Grover's algorithm exponentially reduces the search complexity to square root, which means that AES-128 would provide only 64 bits of security against quantum attacks. At least 256-bit keys are recommended to maintain security.

The threat of quantum attack: impact assessment and strategic readiness

What is quantum computing

Quantum computing represents a different computational paradigm than classical computing. Instead of bits, which represent a 0 or a 1, it uses qubits. Using principles of quantum mechanics such as superposition and entanglement, qubits can represent 0, 1 or a combination of both.

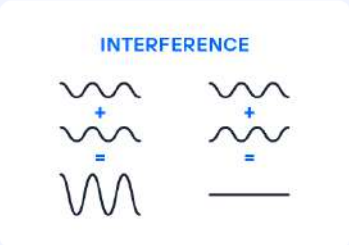
This capability allows quantum computers to process an exponentially greater volume of information than classical computers for certain mathematical problems.

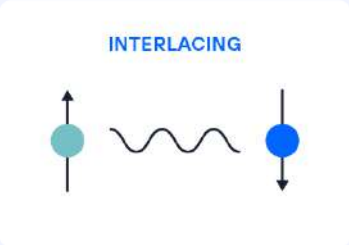
Quantum computing is not universally superior to classical computing. Its advantage lies in its ability to efficiently address problems of high mathematical complexity in domains such as molecular simulation, combinatorial optimization and, of particular relevance to this paper, cryptography.

The National Institute of Standards and Technology (NIST) recommends phasing out RSA-2048 and ECC-256 by 2030, with complete invalidation by 2035. As part of the transition to post-quantum cryptography, NIST urges organizations to migrate to quantum-resistant algorithms before those dates.

Imagine a giant maze where the exit represents the solution to a complex problem, such as deciphering a cryptographic code.

A classical computer would try to solve the maze by trying each path one by one, which could take years if there are millions of possible combinations.





In contrast, a quantum computer can explore multiple paths in parallel, thanks to the **superposition** principle. In addition, **quantum entanglement** allows correlating the results of different quantum states, which makes it easier to find the correct solution more efficiently in certain types of problems.

This means that, in specific cases such **as large integer factorization** (key in RSA) or **discrete logarithm computation** (used in DSA, ECDSA), a quantum computer running **Shor's algorithm** could solve them much faster than any known classical method.

However, not all ciphers are vulnerable. Algorithms based on **post-quantum cryptography** have been designed to resist these attacks, even against quantum computers.

Although quantum computers cannot break all ciphers or solve all problems faster, their quantum parallelism capability **poses a profound challenge to current digital security**, especially for asymmetric cryptography.

Operational implications for businesses

The quantum threat presents a significant strategic and operational risk to any organization, entity or enterprise that relies on cryptography to protect its data and communications. Some of the implications include:

Risks and vulnerabilities

- **Risk of data exposure:** Information encrypted with algorithms vulnerable to quantum computing could be decrypted in the future, compromising sensitive data, trade secrets, intellectual property and confidential communications. This is critical for data with a long-life cycle.

- **Protection against external interference:** Strong encryption is critical to maintain sovereignty over data in storage and in transit, especially in cloud environments. Encryption protects against surveillance and unauthorized access by governments, organizations or cyber criminals.

Operational and strategic challenges

- **Operational disruption:** Replacing current cryptographic systems represents an operational challenge. Migration to post-quantum cryptography will require careful planning, investment and management to avoid service disruptions.

- **Cost of inaction:** Delaying preparation for post-quantum cryptography could result in higher costs in the future, both in remediation of vulnerabilities and potential losses from security breaches.

Key areas of application

- **Critical infrastructure protection:** Post-quantum encryption protects critical infrastructure such as telecommunications, energy and financial systems, safeguarding operational data and control systems.

- **Trusted digital services:** Organizations can offer secure and privacy-friendly digital services by combining post-quantum encryption with AI algorithms, reinforcing their commitment to digital sovereignty.

Key areas of application

- **Critical infrastructure protection:** Post-quantum encryption protects critical infrastructure such as telecommunications, energy and financial systems, safeguarding operational data and control systems.
- **Trusted digital services:** Organizations can offer secure and privacy-friendly digital services by combining post-quantum encryption with AI algorithms, reinforcing their commitment to digital sovereignty.

Strategic implications and business sovereignty in the face of quantum computing

In the context of security based on cryptographic algorithms, quantum computing presents risks and challenges that need to be addressed proactively:

- Common cryptographic algorithms will become vulnerable, putting all protected information at risk. It is essential to prioritize the transition to post-quantum cryptography (PQC), which protects data in the quantum era.
- -The migration to PQC will require investments in technologies, software, hardware and, fundamentally, in staff training to ensure a secure transition.
- Quantum computing must be integrated into the enterprise risk management framework, with regular assessments to identify vulnerabilities and measure progress toward PQC adoption.
- Current regulatory recommendations will evolve toward requirements for resilient cryptography, which demands anticipation and preparation to mitigate risks.
- Crypto-agility will be key to adapting cryptographic systems in the face of new threats and future vulnerabilities.
- Strong cryptographic governance, with full visibility of digital assets, ensures regulatory compliance and efficient implementation.

Digital and technological sovereignty will be crucial at the strategic level to achieving business objectives:

- **Operational sovereignty:** Necessary to optimize efficiency, ensure the security of communications, IoT, AI, and cloud infrastructures.
- **Technology sovereignty:** Vital for resilience and independence of digital infrastructures, as well as for regulatory compliance and operational autonomy.
- **AI and data sovereignty:** Protects national interests, security and privacy, avoiding external influences and ensuring decisions based on reliable information.

Companies should prepare internally and evaluate vendors and third parties to ensure that their external dependencies do not compromise the transition to PQC. Preparing **for Q-Day** (the day when quantum computing will be fully functional) will significantly **reduce costs** and remediation risks if acted upon early.

Post-quantum cryptography (PQC) as a technical and strategic answer

Post-quantum cryptography **(PQC),** or quantum computing-resistant cryptography, involves the development of cryptographic algorithms designed to resist attacks by classical and quantum computers.

However, post-quantum cryptography does not rely on quantum computers. PQC uses classical mathematical algorithms on conventional hardware, while quantum computing uses QKD for key exchange and QRNG to generate random numbers. These algorithms are considered to be resistant to attacks by quantum computers.

PQC to preserve long-term security

PQC is important because information needs to be protected with a long-term confidentiality horizon. It is difficult to predict when there will be a cryptographically relevant quantum computer capable of breaking current cryptography, but the consensus among experts and the NIST forecast is that quantum computing will weaken existing asymmetric cryptography by the end of this decade.

Replacing asymmetric cryptography with quantum-secure cryptography requires proactive action. Migration to PQC must be a priority.

Information encrypted today with vulnerable algorithms could be decrypted in the future with severe consequences because of this. The transition to PQC is therefore not just a technical issue, but a long-term risk management strategy.

Standardization by NIST and other entities

Standardization is key to PQC adoption and interoperability. The US National Institute of Standards and Technology (NIST) has been leading a process of evaluation and standardization of PQC algorithms since 2016.

This process, structured in several rounds, has involved the global cryptographic community in the analysis and evaluation of dozens of proposals. NIST has been the main driver in the identification and standardization of PQC algorithms, through its Post-Quantum Cryptography Project.

Algorithms selected for standardization

NIST published the first post-quantum cryptography algorithms in August 2024, initiating protection against quantum computing. These algorithms, chosen by the global cryptographic community for standardization, allow us to begin the post-quantum transition now:

- **CRYSTALS-Kyber (KEM):** Based on lattice structures and the Learning With Errors (LWE) problem, for general key encapsulation use.
- **CRYSTALS-Dilithium (Digital Signature):** Also based on lattice structures, for general digital signature use.
- **FALCON (Digital Signature):** specifically optimized for reduced signature sizes compared to Dilithium.
- **SPHINCS+ (Digital Signature):** As a hash-based digital signature option, but with a considerably larger signature size.

NIST has published the selection of these first algorithms for official standards for quantum computing-resistant cryptography and is considering standardization of additional algorithms.

Significance of standardization

Standardization of PQC algorithms ensures that the selected algorithms have been evaluated and facilitates the integration of systems and applications, promoting their global adoption by providing:

- **Trust:** the international cryptographic community has evaluated the selected algorithms.
- **Interoperability:** Standardization enables interoperability between different systems and applications.
- **Guidance for adoption:** Provides a clear roadmap for organizations looking to migrate to PQC, enabling them to select algorithms with confidence.

EU role and international participation

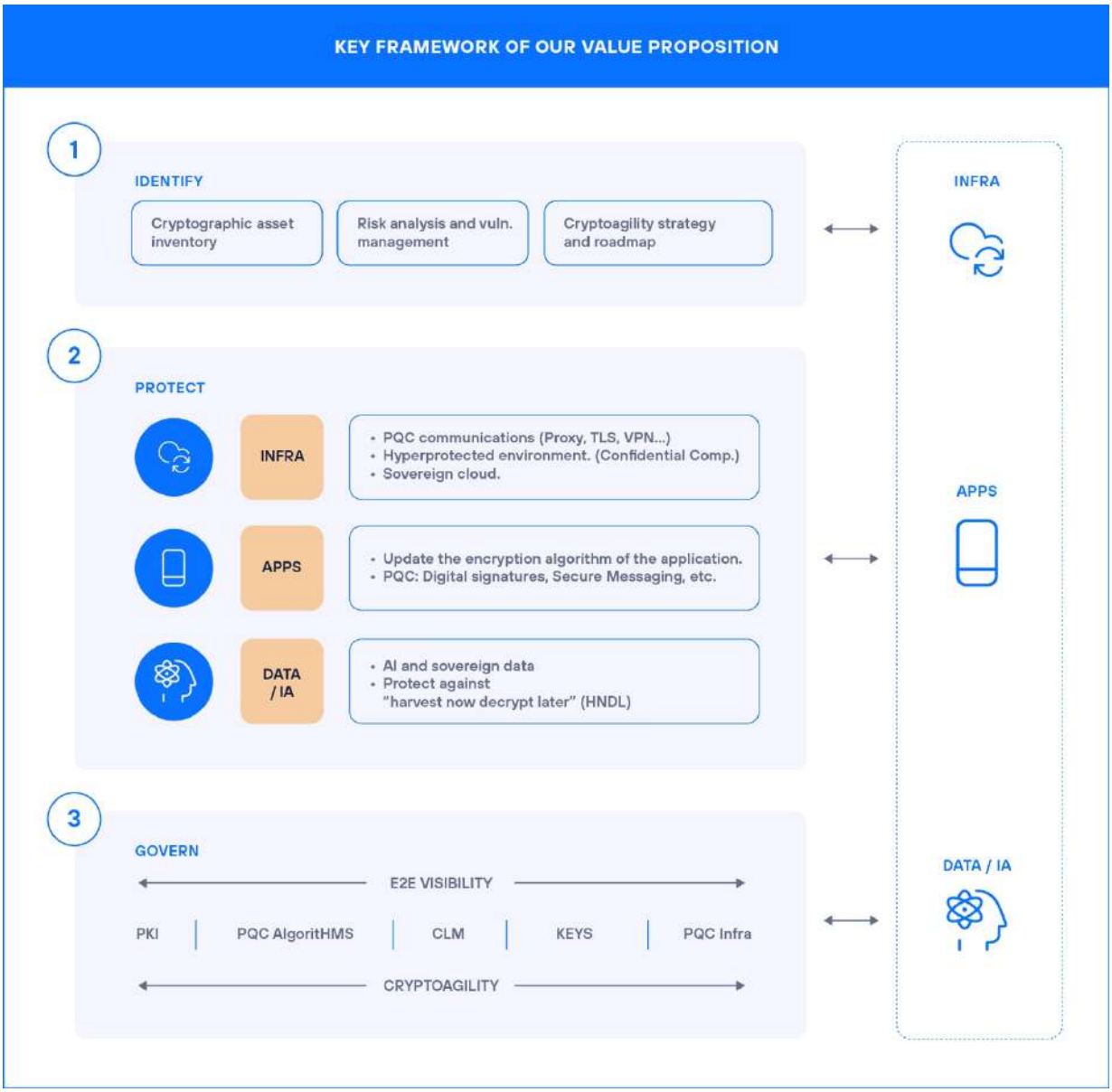
Other organizations, such as ISO and ETSI, are also involved in PQC standardization, ensuring global and coordinated adoption. The European Union Agency for Cyber Security (ENISA) also plays an important role, providing guidance and recommendations on the transition to PQC in the European context.

ENISA works with NIST and other international organizations to promote the adoption of global standards and best practices in post-quantum cryptography. Reports and recommendations on PQC, including algorithm maturity assessments and migration guidelines, have been published.

NIST's standardization of quantum computing-resistant cryptography algorithms marks the beginning of the transition to PQC. Research in post-quantum cryptography continues and it is likely that new algorithms will be developed and standardized.

Pillars for a proactive and gradual transition

The transition to post-quantum cryptography is a complex process that must be approached strategically, in phases and with detailed planning. It is not just a replacement of algorithms, but a progressive redesign of the security infrastructure to ensure resilience to the quantum threat.



The strategy should consider risk assessment, algorithm selection, phased implementation and continuous monitoring, following three pillars: Identify, Protect, and Govern.

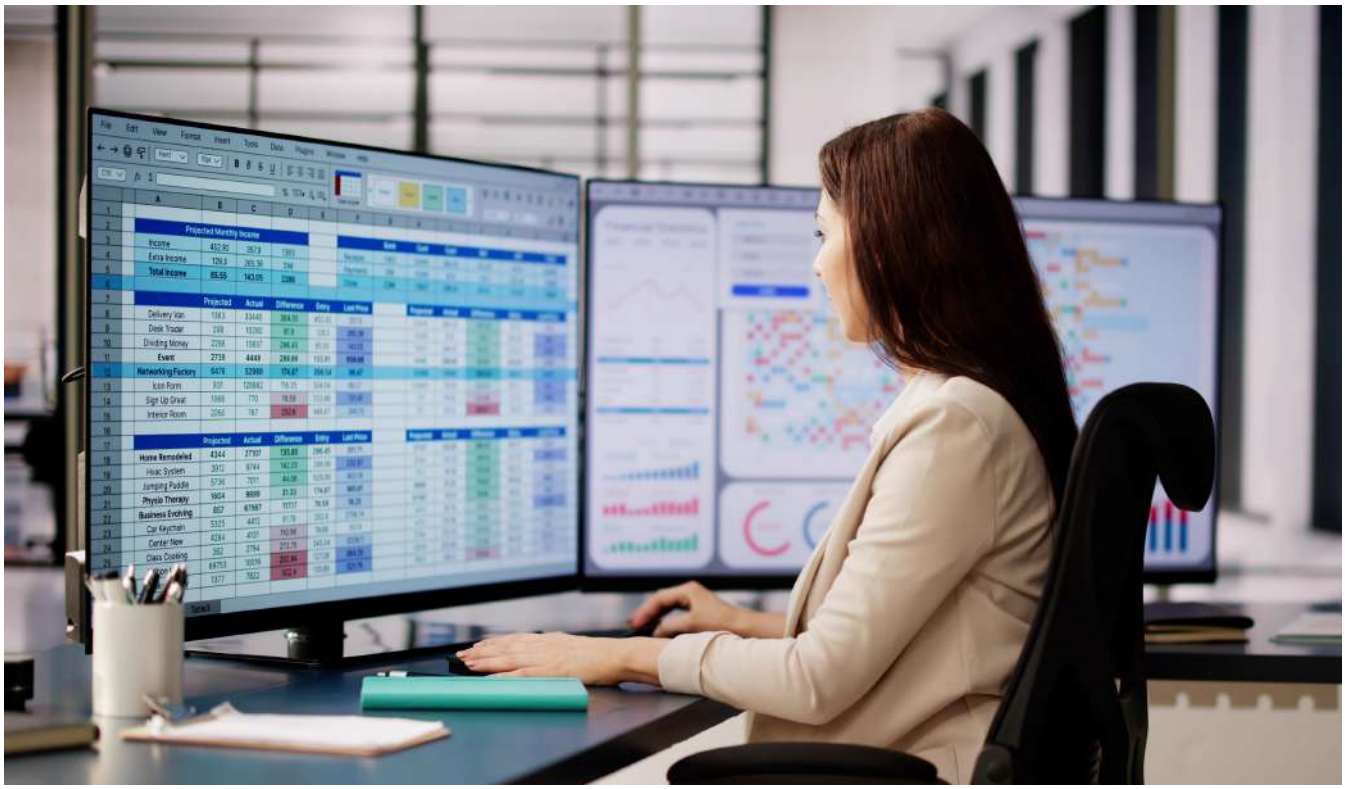
Pillar 1. Identify: Cryptographic inventory and risk assessment

Risk assessment is a continuous and dynamic process that should be integrated into enterprise information security management. It should cover the following key aspects:

Cryptographic asset inventory

The first step is to identify and document all cryptographic assets in the organization to assess their exposure to quantum threat. This includes:

- **Cryptographic keys,** including their type, length and algorithm, used in systems, applications and devices.
- **Digital certificates** identifying their issuer, expiration date, and dependent systems and applications.
- **Cryptographic libraries,** their versions and the applications that use them.
- **External dependencies and third-party services** that use vulnerable cryptography.
- **Cryptographic protocols** used, such as TLS/SSL, SSH, IPsec, etc., including their versions.
- **Context of use** to know what and where it is being used.



Implementing an **automated cryptographic inventory** is critical to understanding the level of risk exposure and prioritizing the migration process to post-quantum cryptography (PQC).

It is recommended that specialized static code analysis and key **discovery tools be used to ensure an accurate and comprehensive assessment of cryptographic assets.**
This analysis should include the **detection of inadequate encryption practices**, such as the use of obsolete cryptographic algorithms, insecure parameters or keys with insufficient key lengths.

Risk analysis and vulnerability management

Once you have a cryptographic inventory, the next step is to assess risks and manage vulnerabilities based on:

- **Dependencies** to determine which systems, applications and business processes relate to each cryptographic asset.
- **Criticality** according to the type of information protected and the impact of its exposure.
- **Vulnerability** to current attacks such as 'Harvest Now, Decrypt Later' and quantum attacks, such as those using RSA or ECC with inadequate key lengths.
- **Priority** to migrate the most critical assets to PQC first according to their risk, probability of occurrence and potential impact.

It is critical to integrate relevant IT sources, such as configuration management systems (CMDB), network logs, and applications, to provide the necessary context for the identified assets. This facilitates a correct correlation between cryptographic assets and their operational dependencies, thus ensuring a more accurate and actionable risk assessment.

At this stage it is critical to align the relevance of PQC with the strategic objectives of the enterprise. Planning must be meticulous, carefully prioritizing what to address first, as changes require significant implementation and adaptation times.

Crypto-agility strategy and roadmap

The risk analysis culminates in an initial transformation plan that should:

- **Define architectural principles** for systems resilient to cryptographic changes, ensuring the ability to replace algorithms agilely.
- **Modernize cryptographic infrastructure** to ensure compatibility and reduce operational risks.
- **Upgrade services and applications** to integrate with PQC cryptography.
- **Implement protection measures** for data in use and at rest, using confidential computing and key lifecycle management technologies.
- **Define a detailed roadmap** with short- and long-term objectives, including specific metrics and targets.

The approach should be progressive, focusing first on critical assets and ensuring operational continuity during the transition.

Telefónica Tech positions itself as a comprehensive partner, capable of providing expert guidance to help organizations define and execute this technology transformation plan. We offer solutions tailored to the specific needs of each company, with extensive experience in the field of crypto-agility and a deep understanding of the strategic objectives of the business.

Organizations, companies, and public administrations ensure that the integration of post-quantum cryptography (PQC) is effective, secure and aligned with business objectives, maximizing the return on investment and strengthening operational resilience.

Pillar 2. Protect: Implementation of solutions and safe transition

Risk assessment is a continuous and dynamic process that must be integrated into a company's information security management. It should cover the following key aspects:

Adoption of prioritized initiatives

PQC implementation requires strategic adoption based on the priorities established during the previous phases.
This process should include:

Pilot and Proof of Concept (PoC)

Prior to full-scale implementation, it is essential to conduct pilot tests in controlled environments to validate transition strategies, considering:

- **Infrastructure:** Testing with different components of the communications infrastructure (such as gateways, VPN tunnels, TLS servers, etc.) to progressively evaluate the integration of post-quantum cryptography algorithms, ensuring compatibility with legacy systems without the need for disruptive changes.
- **Applications:** Use of Cryptography-as-a-Service (Crypto-as-a-Service, CaaS) services to evaluate PQC integration.
- **Data:** Testing with enterprise key management frameworks (EKMF) to protect data at rest and in transit.

Pilot testing should carefully evaluate performance implications, compatibility and potential risks in a controlled environment.

Gradual and progressive implementation

Progressive adoption of PQC ensures a safe transition with minimal operational impact.
It is recommended to:

- Review and adjust pilot test results.
- Migrate critical communications first (VPN, TLS, SSH) using hybrid protocols.
- Modify internal applications with limited impact on services.
- Replace cryptography in front ends exposed to clients.
- Phase out obsolete algorithms in less critical systems.

Re-evaluation and impact

During and after implementation:

- Periodically assess impact in terms of performance and compatibility.
- Update policies and metrics based on experience gained.
- Adjust the transformation plan as new needs or threats emerge.

This iterative process ensures long-term adaptability.

Application scenarios

The transition to post-quantum cryptography demands specific attention to infrastructure, applications and data, addressing quantum threats while fostering digital sovereignty.

Infrastructure

Secure communications

- The use of hybrid algorithms in TLS and the adaptation of communications elements (VPNs, gateways, etc.) with post-quantum cryptography are key to protecting critical communications against future quantum attacks.
- IoT devices must implement lightweight PQC-compliant solutions to ensure performance and security.

Robust infrastructure against quantum attacks

- Incorporate upgradeable hardware security modules (HSMs) to support PQC algorithms.
- Upgrade public key infrastructure (PKI) to handle hybrid certificates.

Sovereign cloud

- Ensure local control of cryptographic keys and data stored within national borders, complying with specific regulations.

Applications

The scope of applications should considerer aspects such as:

- **Post-quantum digital signature:** Implement algorithms such as CRYSTALS-Dilithium or FALCON to ensure the integrity of critical processes and support advanced electronic signatures.
- **Native cryptographic integration:** Upgrade enterprise applications to interoperate with external and modular agile cryptographic solutions.

Data

Data sovereignty is essential to ensure security and regulatory compliance:

Sovereign data protection

- Ensure data is stored and processed under specific jurisdictions.
- Apply post-quantum cryptography both in transit and at rest, integrating local key management resistant to quantum attacks. This not only mitigates threats such as Harvest Now, Decrypt Later, but also ensures data sovereignty by maintaining exclusive control of keys without relying on third parties or external environments.

These scenarios ensure a holistic approach that protects assets, optimizes resources and fosters digital autonomy during the transition to PQC.

Performance impact and IoT-specific considerations

The transition to PQC will impact system performance due to the increased computational complexity of post-quantum algorithms. This impact needs to be assessed and mitigated by:

- **Selection of optimized algorithms** that balance safety and efficiency to maintain system performance during the transition.
- Optimized software and hardware implementations for a smoother and more efficient transition.
- **Use of specific cryptographic accelerators** to optimize the execution of cryptographic algorithms and improve execution times.
- **Hybrid architectures combining classical and post-quantum cryptography** while completing the transition to gradually incorporate the new PQC algorithms, while maintaining existing systems

Pillar 3. Governance: Implementation and ongoing monitoring

Governance lays the foundation for managing the transition to post-quantum cryptography in a structured and efficient manner. This stage seeks to implement the necessary capabilities to ensure cryptographic security in the long term, adapting to technological changes and aligning with business objectives.

Governance includes internal coordination and interoperability with existing systems. This allows the cryptographic infrastructure to be continuously adjusted and improved.

La gobernanza incluye la coordinación interna y la interoperabilidad con sistemas existentes. Esto permite ajustar y mejorar la infraestructura criptográfica de manera continua.

Cryptographic Center of Excellence

It is recommended to establish a Cryptographic Center of Excellence (CCoE) or a dedicated team responsible for:

- Keep up to date with developments in quantum computing and PQC, as research in both fields is ongoing.
- **Assess the potential impact of quantum computing** on the company considering various scenarios and timelines.
- Define and keep up to date the company' s cryptographic policy, including the transition to PQC.
- **Identify critical assets that require priority migration,** including vulnerable systems and data that need urgent migration to PQC.

Telefónica's Cryptography Center of Excellence (CCoE) has implemented advanced cryptographic strategies to protect its digital assets. It focuses on three areas: communications and cyber security, computing and simulation, and sensing and metrology to leverage quantum computing and improve the security of the company's networks and systems and its customers.

This team manages and secures the company's cryptographic keys, leads the adoption of PQC technologies and develops internal regulations to implement a crypto-agility strategy to protect systems and infrastructures.

Telefónica's CCoE also collaborates with regulators and participates in global initiatives and ensures that the company is ready to face future quantum threats and comply with the most stringent security standards.

End-to-end visibility

End-to-end visibility (E2E) in cryptography is critical to minimize risk, control the attack surface and facilitate strategic, tactical and policy decisions. It provides a comprehensive view of all cryptographic assets, such as keys, certificates, libraries and protocols.

Key components of E2E visibility

- **Automated discovery tools:** Identify cryptographic assets and detect misconfigurations, use of obsolete algorithms or vulnerable keys.
- **Centralized and modular management of cryptographic assets:** Enables early detection of vulnerabilities and facilitates rapid response to threats.
- **Integration with security systems (SIEM, SOAR):** Links cryptographic visibility with management platforms to correlate events and analyze risks.
- **Continuous monitoring:** Ensures cryptographic assets are up-to-date and secure while detecting new risks.

Key benefits

- **Proactive risk control:** Identifies and addresses critical priorities.
- **Resource optimization:** Centralizes management to reduce duplication and improve resource allocation.
- **Strategic support:** Provides accurate information to plan investments and make informed decisions.

End-to-end visibility is the basis for implementing robust security measures and ensuring transparency in cryptographic management.

Crypto-agility

Crypto-agility ensures the ability to quickly adapt to new threats and changes in cryptographic standards without compromising operability.

This approach also includes managed services and incident response for comprehensive security management.

Managed Servies

- **Cryptographic centralization:** Implementing Cryptography as a Service (CaaS) facilitates cryptographic operations using standard API interfaces.
- **Process automation:** Includes the management of keys, certificates and algorithms to avoid manual errors.
- **Managed complex scenarios:** Efficient handling of identities and cryptography in hybrid or distributed environments.

Incident response

The ability to manage cryptographic incidents in an agile manner is critical to mitigate risks. This involves:

- **Specific response plans:** Clear procedures to identify, contain and mitigate PQC-related incidents.
- **Incorporation of crypto-agility:** Enables rapid algorithm updates in case of vulnerabilities.
- **Drills and training:** Conduct periodic drills to assess the readiness and effectiveness of the response plan.

Key benefits of crypto-agility

- **Seamless Compatibility:** Protection of applications and networks without the need to modify code or revise fundamental architectures.
- **Long-term interoperability:** Hybrid PKI support and modular architecture to facilitate future changes without operational disruption.
- **Operational resilience:** The integration of crypto-agility into systems ensures constant updating in the face of new threats.

Crypto-agility enables organizations to stay protected against vulnerabilities and new threats without affecting their operational capacity.

Industry use cases

The threat of quantum computing and the need for post-quantum cryptography are not abstract: they have concrete and significant implications for a variety of industries. Some examples:

Financial sector

- **Threat:** Financial institutions (banks, stock exchanges, insurance companies) rely heavily on cryptography to protect transactions, customer information and financial assets.
- PQC applications:
- **Secure communications:** Protecting communications between banks, customers and other financial institutions using TLS/SSL with PQC algorithms.
- **Digital signatures:** Ensuring the integrity and authenticity of financial transactions using PQC digital signatures.
- **Blockchain and cryptocurrencies:** Blockchain networks and cryptocurrencies using vulnerable cryptographic algorithms such as ECDSA or RSA should migrate to PQC algorithms such as Dilithium to maintain their security.
- **Data-at-rest protection:** Encryption of databases and files containing sensitive financial information using PQC algorithms.
- **Compliance:** Financial regulations (such as PCI DSS, PSD2 in Europe, and other regulations) will increasingly require the use of cryptography that is resistant to quantum computing.

Health sector

- **Threat:** Hospitals, clinics, health insurance companies, and laboratories handle large amounts of confidential medical information (medical records, genomic data, test results).

  Exposure of this information could have serious consequences for patients' privacy and the institutions' reputation.

- **PQC applications:**
  - **Electronic Health Record (EHR) protection:** EHR encryption using PQC algorithms to protect confidentiality of patient information.

  - **Secure communications:** Protection of communications between physicians, patients and other healthcare professionals (telemedicine, secure e-mail) using TLS/SSL with PQC algorithms.
  - **Secure information exchange:** Facilitating the secure exchange of medical information between different institutions using PQC-compliant protocols and data formats.
  - **Genomic research:** Protection of genomic data, which are highly sensitive, such as national genomic nodes, and have a long-term value, using PQC algorithms.
- **Compliance:** Regulations such as HIPAA in the U.S. and GDPR in Europe require the protection of medical information. PQC will be essential to comply with these regulations in the quantum era.

Government and defense sector

- **Threat:** Governments and defense agencies handle high-value classified information, including state secrets, military communications or intelligence data.

  Exposure of this information could have devastating consequences for national security.
- PQC applications:
  - **Classified communications:** protection of classified communications (voice, data, video) using PQC algorithms.
  - **Centralized management of cryptographic keys:** Classical and post-quantum cryptographic keys are essential for security and crypto-agility.
  - **Encryption of data at rest:** Encryption of databases and files containing classified information using PQC algorithms.
  - **Defense systems:** Ensuring the integrity and authenticity of defense systems and other critical systems using PQC digital signatures.
  - **Critical infrastructure:** Protecting critical infrastructure (power grids, transportation systems, etc.) against quantum attacks using PQC.
- **Compliance:** Governments and defense agencies will adopt PQC because of the need to protect national security.

Automotive sector

- **Threat:** Modern vehicle systems are highly software-dependent, with internal and external communications.

  A cyberattack could compromise occupant safety..
- **PQC applications:**
  - **V2V and V2I communications:** Protection of Vehicle-to-Vehicle and Vehicle-to-Infrastructure communications to ensure data integrity and prevent malicious attacks.
  - **Software updates:** The integrity of updates must be ensured to prevent malicious modifications.

Industry 4.0

- **Threat:** Industry 4.0 makes extensive use of IoT in all its processes. These devices are typically low-resource, low-compute-capacity devices operating in complex environments.

- **PQC applications:**
  - **M2M communications:** Securing machine-to-machine communications.
  - **Supply chain control:** Ensuring the integrity of processes.

Conclusions and recommendations for securing the digital future in the quantum era

This paper has explored the imminent threat of quantum computing to current cryptography, the critical need for post-quantum cryptography, and the strategies needed for a secure and effective transition.

Need for action

The transition to post-quantum cryptography is an immediate need, due to three fundamental reasons:

- **Cryptography as a pillar of digital sovereignty:** In an increasingly interconnected and changing digital environment, cryptography not only guarantees the confidentiality and integrity of information but is a key element in preserving technological autonomy and sovereignty over data. Faced with the threat posed by future quantum computers, the adoption of post-quantum cryptography (PQC) becomes strategic to avoid reliance on vulnerable or third-party controlled technologies and thus ensure full and resilient control over critical digital assets.

- **The real threat of quantum computing:** current algorithms such as RSA and ECC could be compromised in less than a decade due to advances in quantum computing, highlighting the importance of acting now to protect sensitive and confidential information.

- **Post-quantum cryptography as a solution:** offers algorithms capable of resisting both classical and quantum computers, implementable today with conventional technology, thus reducing the window of vulnerability to future attacks.

Given this context, the urgency in adopting post-quantum cryptography is undeniable.

Key recommendations and effective actions

The following recommendations delve into essential strategies to ensure a robust digital future in the quantum age. Organizations should focus on:

- **Continuous assessment and management of cryptographic risk,** establishing a comprehensive, automated and up-to-date cryptographic inventory.

- **Gradual implementation and crypto-agility,** adapting modular technology architectures to enable rapid changes of cryptographic algorithms, thus facilitating continuous adaptation to future threats.
- **Strengthening cryptographic governance,** through the creation of a Cryptographic Center of Excellence (CCoE), ensuring leadership and oversight of the transition to PQC, as well as current and future regulatory compliance.

It is further recommended to develop a detailed transformation plan based on risk assessment, conduct pilot tests prior to full-scale implementation and ensure continuous training of personnel involved in this strategic transition.

It is recommended to start today to ensure an effective transition to post-quantum cryptography: with a risk assessment, a cryptographic inventory, and pilot testing with NIST-standardized PQC algorithms. Crypto-agility is essential.

About Telefónica Tech

Telefónica Tech is the leading company in digital transformation. It offers a wide range of integrated technological services and solutions in Cyber Security, Cloud, IoT, Big Data, Artificial Intelligence and Blockchain.

telefonicatech.com

2025 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

The information contained in this document is the property of Telefonica Cybersecurity & Cloud Tech S.L.U. (hereinafter "Telefónica Tech") and/or any other entity within the Telefónica Group or its licensors.

Telefónica Tech and/or any Telefónica Group company or Telefónica Tech's licensors reserve all intellectual property rights (including any patents or copyrights) arising from or pertaining to this document, including the rights to design, produce, reproduce, use and sell this document, except to the extent that such rights are expressly granted to third parties in writing.

The information contained herein may be subject to change at any time without notice.

Telefónica Tech shall not be liable for any loss or damage arising from the use of the information contained herein.
Telefónica Tech and its trademarks (as well as any trademarks belonging to the Telefónica Group) are registered trademarks. Telefónica Tech and its subsidiaries reserve all rights therein.

This report is published under a Creative Commons Attribution - Share license.

Telefónica Tech