NIST Towards Post-Quantum Cryptography - Against Invaders - Notícias d

Data: 2025-09-29 05:08:55

Autor: Inteligência Against Invaders

Marcello Filacchioni**:29 September 2025 07:08**

NIST , through its *National Cybersecurity Center of Excellence (NCCoE)* , has released the first draft of a new document dedicated to **post-quantum cryptography (PQC)** .

Cryptographic algorithms have always protected our most sensitive digital data from unauthorized access. So far, they've worked well, as even the most powerful computers haven't been able to break them. But a challenge looms on the horizon: **quantum computers** , which could one day break traditional algorithms and expose information currently considered secure.

This requires **new algorithms** that can withstand both current and future quantum computers. This is where **PQC** , or "quantum-resistant" cryptography, comes in. The NCCoE project, called *Migration to PQC* , was created precisely to help companies and institutions plan and test this transition.

Why act now?

While we don't know when truly powerful quantum computers will arrive (some experts say within 10 years), it's worth starting now. Historically, it takes a long time to move from a new algorithm to its full adoption in information systems.

Furthermore, there is a concrete risk known as **"harvest now, decrypt later"** : an attacker can collect large amounts of encrypted data today, store it, and wait until a quantum computer can decrypt it one day. This could compromise sensitive and long-lived information even if it appears secure today.

The content of the document

The new *white paper* (CSWP 48) helps organizations understand **how to connect PQC migration with existing risk management practices** . Specifically, it correlates the capabilities demonstrated in the NCCoE project with two key and well-known NIST documents:

- The **Cybersecurity Framework 2.0 (CSF 2.0)** , used worldwide to manage cyber risks.
- The **SP 800-53 catalog** , which collects the security and privacy controls to protect information systems.

The goal is to help organizations plan their migration to post-quantum cryptography in an orderly manner, aligning new efforts with established practices and identifying the most appropriate security

controls.

NIST will collect comments on this draft through October 20, 2025, via the NCCoE project page.

Marcello Filacchioni
ICT CISO and Cyber Security Manager with over twenty years of experience in the public and private sectors, he has led IT security projects for leading companies. Specialising in risk management, governance and digital transformation, he has collaborated with international vendors and innovative start-ups, contributing to the introduction of advanced cybersecurity solutions. He holds numerous certifications (CISM, CRISC, CISA, PMP, ITIL, CEH, Cisco, Microsoft, VMware) and teaches pro bono in the field of cyber security, combining his passion for technological innovation with his commitment to spreading the culture of digital security.

Lista degli articoli