MARSH

Facing Quantum Risks Today with PQC

A computação quântica abre oportunidades em materiais, energia, finanças e medicina, mas também cria um risco direto para a segurança da informação. Algoritmos como Shor e Grover já estão mudando o cenário da infosegurança: o “Q-day” pode tornar vulneráveis os esquemas criptográficos atuais e habilitar estratégias de “colher agora, descriptografar depois”. Para a Diretoria, a prioridade é inventariar dados sensíveis, identificar sistemas que utilizam criptografia ou assinatura digital e planejar a transição para criptografia pós-quântica antes que se torne urgente.

1

Quantum é oportunidade e ameaça
Pode acelerar avanços em materiais, energia, finanças e medicina, mas também pressiona a segurança da informação criptografada.

2

Q-day exige anticipación
Expertos citados estiman que podría haber ocurrido ya (15%) o suceder antes de 2035 (34%). El riesgo “harvest now, decrypt later” ya cuenta hoy.

3

Criptografia atual sob pressão
Shor y Grover cambian el panorama de infoseguridad. La organización debe identificar dónde depende de algoritmos vulnerables.

4

A transição pós-quântica já começou
Padrões como FIPS 203, FIPS 204 e FIPS 205 indicam o caminho para algoritmos resistentes à computação quântica.

5

Roteiro para a diretoria
Inventariar dados sensíveis em 2026, mapear componentes criptográficos em 2027 e planejar implementações pós-quânticas até 2030.