Comunicado de imprensa

**Microsoft anuncia*****Quantum Safe Program Strategy* para garantir resiliência na era da computação quântica**

**Lisboa, 04 de setembro de 2025** – A Microsoft anuncia a [*Quantum Safe Program Strategy*](https://aka.ms/QSP/Strategy-2025) — um passo significativo na preparação para a era da computação quântica, com uma mentalidade de segurança em primeiro lugar. A estratégia da Microsoft define como pretende permitir a adoção precoce de capacidades pós-quânticas nos seus produtos e serviços até 2029 e completar a transição até 2033, dois anos antes da maioria dos prazos estabelecidos pelos governos para a conclusão desta transição.

A computação quântica [promete avanços significativos na medicina, nas ciências dos materiais](https://blogs.microsoft.com/on-the-issues/2025/04/28/investing-in-american-leadership-quantum/) e muitas outras áreas, mas à medida que a tecnologia evolui, também a abordagem à cibersegurança deve evoluir. A tecnologia quântica introduz novas oportunidades, mas também novos riscos, sobretudo para a segurança da informação. Para proteger dados sensíveis e manter a confiança pública nos sistemas digitais que sustentam as economias e sociedades, os governos devem facilitar uma transição criptográfica antes de os computadores quânticos se tornarem amplamente disponíveis.

Durante décadas, os algoritmos de encriptação protegeram tudo, desde palavras-passe pessoais e comunicações privadas até às infraestruturas críticas que suportam o sistema financeiro global. No entanto, um computador quântico suficientemente poderoso poderá, um dia, tornar obsoletos alguns métodos de encriptação, colocando em risco a confidencialidade e a integridade dos dados que sustentam a vida digital dos utilizadores.

**A indústria e os governos devem agir rapidamente para tornar a infraestrutura digital mundial segura face à computação quântica**

Embora os especialistas prevejam que estas capacidades quânticas apenas [surjam na década de 2030](https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/), a necessidade de transitar para uma criptografia pós-quântica é imediata. Esta transição é complexa, exigindo tempo e recursos, e as organizações que não agirem de imediato poderão, em breve, ver as suas informações mais sensíveis expostas.

Entretanto, uma ameaça real já se começa a materializar: atores maliciosos podem recolher dados encriptados hoje, com a intenção de os desencriptar no futuro através de computadores quânticos — uma tática conhecida como *“harvest now, decrypt later*”. Isto reforça a necessidade de agir o quanto antes para proteger a informação sensível, antes que as ameaças quânticas se tornem realidade.

**Aposta em parcerias é crucial para garantir um futuro pós-quântico seguro**

A transição do ecossistema digital exige colaboração em escala global. A Microsoft contribui para múltiplas iniciativas que visam facilitar esta transição, incluindo o [Projeto de Criptografia Pós-Quântica do NIST](https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization), o [Centro Nacional de Excelência em Cibersegurança para a Migração para Criptografia Pós-Quântica](https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms), o [Internet Engineering Task Force (IETF)](https://datatracker.ietf.org/wg/pquip/about/), o [projeto Open Quantum Safe (OQS)](https://openquantumsafe.org/) e a  [Post-Quantum Cryptography Coalition](https://www.mitre.org/news-insights/news-release/post-quantum-cryptography-coalition-launches) da MITRE.

Através destes esforços, a Microsoft [ajuda a desenvolver algoritmos pós-quânticos](https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/), [apoia a sua adoção em normas como TLS e X.509](https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-comes-to-windows-insiders-and-linux/4413803) e promove a aceleração da sua implementação tanto em tecnologias comerciais como de código aberto. Recentemente[, a empresa lançou capacidades de criptografia pós-quântica de forma antecipada para alguns utilizadores de Windows e Linux](https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-comes-to-windows-insiders-and-linux/4413803), permitindo testar estas funcionalidades e identificar potenciais desafios.

A indústria privada não pode, sozinha, resolver estes desafios. Os governos desempenham um papel crítico em viabilizar um futuro pós-quântico seguro, através de uma colaboração sólida com a indústria e da implementação de políticas eficazes. Para acelerar esta preparação, a Microsoft recomenda que os governos adotem as seguintes medidas:

* **Estabelecer a segurança pós-quântica como prioridade nacional de cibersegurança:** posicionar a criptografia pós-quântica como uma prioridade estratégica e integrá-la nos quadros nacionais de cibersegurança.
* **Alinhar estratégias pós-quânticas entre jurisdições:** harmonizar políticas públicas, normas e cronogramas de transição. O G7 deve liderar, expandindo a sua linha de trabalho sobre criptografia pós-quântica no setor financeiro, de forma a alinhar as estratégias mais amplas de segurança quântica dos Estados-membros.
* **Adotar normas internacionais:** apoiar o desenvolvimento de padrões globais e evitar abordagens fragmentadas e regionais, que prejudiquem a interoperabilidade, a inovação e a segurança.
* **Definir cronogramas antecipados e progressivos:** impulsionar a ação antes de 2030. Por exemplo, a Política 15 do CNSS dos EUA exige algoritmos pós-quânticos em todos os novos produtos e serviços destinados a sistemas de segurança nacional a partir de janeiro de 2027.
* **Liderar através do exemplo com planos de transição transparentes:** publicar e atualizar regularmente os planos de transição dos governos — incluindo cronogramas, marcos e orçamentos — para fomentar a partilha de conhecimento e de boas práticas.
* **Sensibilizar e reforçar competências na força de trabalho:** educar o público e os setores de infraestruturas críticas sobre os riscos e a preparação quântica. Investir em programas de capacitação que dotem a força de trabalho das competências necessárias para a transição pós-quântica.

A transição para um mundo digital seguro face à computação quântica requer uma colaboração estreita entre a indústria e os governos para ser bem-sucedida. Neste sentido, a Microsoft apresenta a sua estratégia de transição para orientar decisores políticos e clientes relativamente aos seus planos, incentivando outros a agir, e mantém-se disponível para colaborar com legisladores em todo o mundo, facilitando a transição do ecossistema digital de forma mais ampla.

**CONTACTOS**

|  |  |  |
| --- | --- | --- |
| **Catarina Brito** | **Inês Filipe** |  |
| catarina.brito@lift.com.pt  | ines.filipe@lift.com.pt |  |
| 914 310 661 | 910 283 054 |  |

**SOBRE A MICROSOFT**

Microsoft (Nasdaq "MSFT" @microsoft) cria plataformas e ferramentas robustecidas por Inteligência Artificial para entregar soluções inovadoras que correspondam às necessidades crescentes dos nossos clientes. Enquanto empresa de tecnologia está comprometida com a democratização do acesso a Inteligência Artificial de forma responsável, mantendo a missão de capacitar todas as pessoas e organizações no planeta para atingir mais.