DELL Technologies

White paper

Criptografia pós-quântica: preparando-se para a era quântica

White paper da Dell Technologies

Sumário

Visão geral executiva

A computação quântica está mudando rapidamente da pesquisa teórica para a realidade prática. Antes considerado um horizonte distante, os avanços em hardware, algoritmos e investimentos estão acelerando a chegada de máquinas capazes de resolver problemas que os computadores tradicionais não conseguem. As implicações para o setor são profundas. Da descoberta de medicamentos à modelagem climática e logística global, a computação quântica promete desbloquear inovações que antes estavam fora de alcance.

Mas esse avanço vem com um desafio disruptivo: os computadores quânticos comprometerão as fundações criptográficas que protegem a economia digital. A criptografia de chave pública, algoritmos como RSA e criptografia de curva elítica (ECC), protegeu as comunicações digitais, os sistemas financeiros, os registros de saúde e as seguranças nacionais por décadas. Esses métodos dependem de problemas matemáticos que não são gerenciáveis para computadores clássicos. No entanto, com o advento dos computadores quânticos criptograficamente relevantes (CRQCs), esses mesmos problemas podem ser resolvidos com eficiência, tornando a segurança atual obsoleta.

Essa ameaça não é teórica. Algumas organizações já estão usando uma tática conhecida como "coletar agora, descriptografar depois" (HNDL) — coletando dados criptografados hoje com a expectativa de quebrá-los quando os computadores quânticos amadurecerem. As informações confidenciais que parecem seguras agora podem estar vulneráveis em questão de anos. O momento de agir não é quando os CRQCs chegarem, é agora.

Este white paper explica a urgência da ameaça quântica, explora o campo emergente da criptografia pós-quântica (PQC) e fornece orientação sobre como as organizações podem se preparar. Ele destaca o compromisso da Dell Technologies em construir um futuro seguro com a computação quântica, incorporando a segurança em toda a cadeia de suprimentos, hardware, firmware, software e rede de parceiros, alinhando-se aos padrões de criptografia pós-quântica (PQC) do NIST — FIPS 203, FIPS 204 e FIPS 205 — e com as diretrizes do Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). O objetivo da Dell é claro: garantir que a inovação possa avançar sem sacrificar a segurança ou a confiança.

Terminologia

Ao longo deste documento, você encontrará uma série de termos. Nós tentamos delinear alguns desses termos para ajudar na compreensão do artigo.

Criptografia pós-quântica: uma nova abordagem matemática para a criptografia, com novos algoritmos, destinada a ser segura contra ataques de computadores quânticos. Esses algoritmos são executados em computadores clássicos e são resistentes tanto ao ataque quântico quanto aos ataques clássicos de criptografia conhecidos.

Resiliente à computação quântica — Refere-se a sistemas, algoritmos ou infraestruturas projetados para permanecer seguros mesmo na presença de computadores quânticos criptograficamente relevantes (CRQCs). Um sistema resiliente ao ataque quântico utiliza criptografia pós-quântica (PQC) ou outras proteções que resistem a ataques tanto clássicos quanto quânticos, garantindo a confidencialidade, a integridade e a autenticidade dos dados no futuro. Outros termos, como resiliente à computação quântica e seguro para o ambiente quântico, também são usados de forma intercambiável.

Agilidade criptográfica — (também conhecida como agilidade criptográfica) é a capacidade dos sistemas e aplicativos de uma organização de mudar rapidamente e sem problemas algoritmos criptográficos, protocolos ou comprimentos de chave sem precisar de grandes reformulações ou interrupções operacionais.

"Harvest Now, Decrypt Later" (HNDL), ou "Coletar agora, descriptografar depois", também conhecido como "Record Now, Decrypt Later" (Gravar agora, descriptografar depois), é o ato de adversários coletarem e armazenarem dados criptografados hoje com a intenção de descriptografá-los no futuro assim que os computadores quânticos criptograficamente relevantes (CRQCs) estiverem disponíveis.

Computação quântica e a ameaça à criptografia

A ascensão da computação quântica

Como descrevemos em nosso post do blog há quase um ano, Criptografia pós-quântica: um imperativo estratégico para resiliência empresarial, do nosso CTO John Roese, os computadores clássicos, seja em notebooks, smartphones ou servidores, processam informações usando bits, que existem em um estado de zero ou um. Esse modelo binário impulsionou décadas de progresso, mas limita a forma como as informações podem ser representadas e manipuladas. Os computadores quânticos usam qubits, que podem existir em vários estados simultaneamente por meio de princípios como superposição e emaranhamento. Isso permite que as máquinas quânticas explorem um grande número de soluções possíveis em paralelo, proporcionando uma vantagem computacional para classes específicas de problemas.

As possíveis aplicações da computação quântica são extraordinárias. Os pesquisadores antecipam avanços em produtos farmacêuticos simulando interações moleculares com precisão que os computadores clássicos não conseguem alcançar. Os cientistas do clima vislumbram modelos mais precisos de sistemas globais, enquanto o setor de energia vê potencial para otimizar as redes de energia e o armazenamento. Até mesmo a logística e a fabricação podem se beneficiar das técnicas de otimização quântica. Os benefícios são reais e alcançáveis, mas os riscos também estão presentes.

Por que a criptografia está em risco

A criptografia sustenta a confiança na era digital. Quando você insere um número de cartão de crédito, faz login em um site seguro ou recebe uma atualização de software assinada, a criptografia garante confidencialidade, autenticidade e integridade. A maior parte dessa proteção depende de criptografia de chave pública — algoritmos como RSA e ECC que são baseados em problemas matemáticos considerados computacionalmente inviáveis para máquinas clássicas.

A computação quântica muda essa equação. Usando o **Algoritmo de Shor,** um computador quântico suficientemente poderoso pode resolver os problemas de fatoração e logaritmo discreto que dão força à RSA e ao ECC. Quando os CRQCs existirem, as assinaturas digitais que protegem as atualizações de software, as chaves que estabelecem sessões TLS e os certificados que autenticam dispositivos podem ser comprometidos. O impacto é sistêmico, ameaçando os próprios mecanismos que garantem a segurança das transações digitais.

A criptografia simétrica, algoritmos como AES usados para proteger dados armazenados ou comunicações seguras, enfrenta um desafio diferente, embora menos grave. O **Algoritmo de Grover** permite que um computador quântico reduza a força efetiva das chaves simétricas, reduzindo efetivamente sua segurança para metade. Embora isso possa ser mitigado com a mudança para tamanhos de chave maiores, como AES-256, o ajuste ressalta o alcance generalizado das ameaças quânticas

Urgência e consequências

As consequências vão muito além do risco teórico. As organizações que não conseguem se preparar enfrentam a exposição de propriedade intelectual confidencial, interrupção de sistemas financeiros, violações de dados de saúde e ameaças à segurança nacional. A estratégia "Coletar agora, descriptografar depois" aumenta a urgência: os adversários só precisam capturar dados criptografados hoje e esperar pelos meios para descriptografá-los. Quando os CRQCs chegarem, o dano já será irreversível.

Criptografia pós-quântica e padrões emergentes

Definição da criptografia pós-quântica

A criptografia pós-quântica (PQC) refere-se a uma nova geração de algoritmos projetados para proteger sistemas digitais contra ataques clássicos e quânticos. Ao contrário da distribuição de chaves quânticas, que requer hardware especializado, o PQC foi projetado para ser executado na infraestrutura clássica atual — servidores, endpoints, redes — tornando-o a maneira mais prática e escalável de se preparar para a era quântica.

A base do PQC é um conjunto de problemas matemáticos que, segundo o melhor conhecimento atual, são resistentes a técnicas quânticas, como os algoritmos de Shor e Grover. A criptografia baseada em reticulados, as assinaturas baseadas em hash, os esquemas baseados em código e as equações multivariadas representam as famílias mais promissoras. Essas abordagens estão sendo rigorosamente testadas e padronizadas para garantir que forneçam a mesma confiabilidade e interoperabilidade que a RSA e o ECC já entregaram.

O esforço global de padronização — Padrões emergentes do setor

Ao reconhecer a urgência da ameaça, os governos e órgãos de padronização fizeram do PQC uma prioridade global. O Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) lançou seu projeto PQC em 2016, convidando a comunidade de pesquisa criptográfica a propor, analisar e refinar algoritmos candidatos. Após anos de testes, o NIST anunciou o primeiro grupo de algoritmos padronizados em agosto de 2024:

- **CRYSTALS-**Kyber para criptografia de chave pública e estabelecimento de chaves
- **CRYSTALS-**Dilithium e SPHINCS para assinaturas digitais

Os algoritmos adicionais permanecem em análise para fornecer diversidade e flexibilidade para diferentes necessidades de implementação, incluindo sistemas leves, como firmware incorporado. Esse processo de padronização em evolução garante que as organizações em todo o mundo tenham um caminho claro para adotar soluções resistentes à computação quântica.

Padrões do NIST — FIPS 203, 204, 205

Em agosto de 2024, o Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) finalizou os primeiros algoritmos de PQC:

- FIPS 203 (ML-KEM) — Baseado em CRYSTALS-Kyber, um mecanismo de encapsulamento chave. Fornece segurança IND-CCA2, o que significa que os textos cifrados permanecem indistinguíveis mesmo sob ataques adaptativos de texto cifrado escolhido.
- FIPS 204 (ML-DSA) — Baseado em CRYSTALS-Dilithium, um algoritmo de assinatura digital. Oferece segurança sólida de EUF-CMA (inexistência de falsificação existencial sob ataques de mensagens escolhidas), que é o requisito padrão para assinaturas digitais.
- FIPS 205 (SLH-DSA) — Baseado em SPHINCS+, um esquema de assinatura baseado em hash. Selecionado como fallback conservador, não dependente de problemas de reticulados.

Um roteiro obrigatório

Ao perceber a importância de adotar algoritmos de criptografia resistentes à computação quântica, o governo federal dos EUA começou a emitir requisitos de PQC para agências federais. Isso inclui os seguintes requisitos: National Security Memorandum 10 (NSM-10), Commercial National Security Algorithm Suite (CNSA 2.0), National Institute of Standards and Technology (NIST) Interagency Report (IR) 8547, e Office of Management and Budget Memorandum 23-02 (OMB M-2302), além de outros.

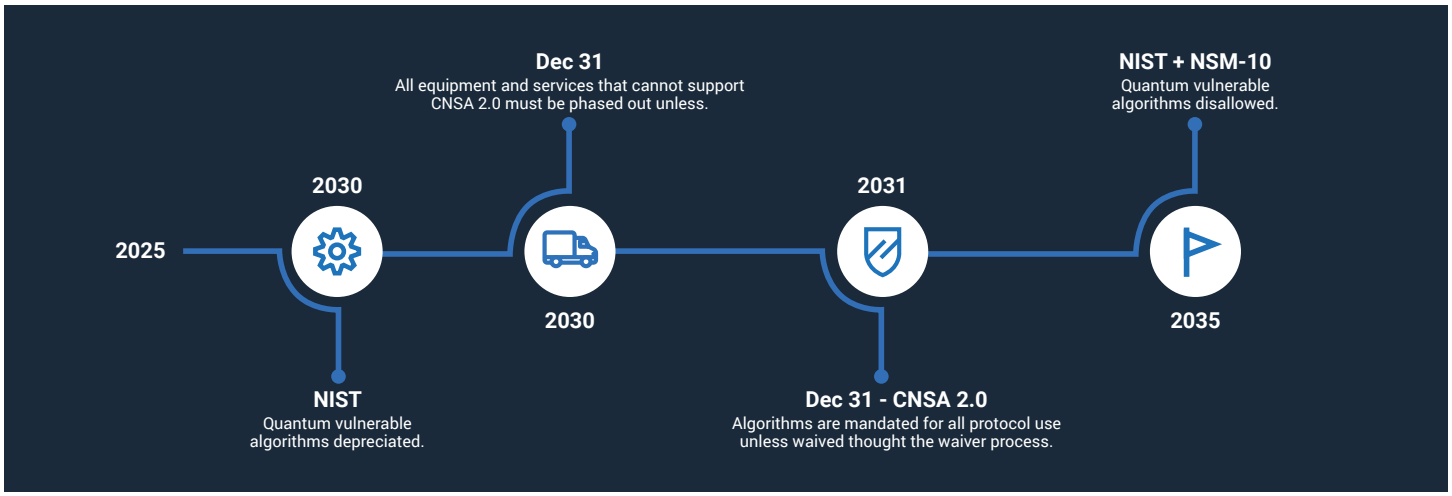
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodogies.

Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)
Introduces the first recommendations post-quantum cryptographic algorithms

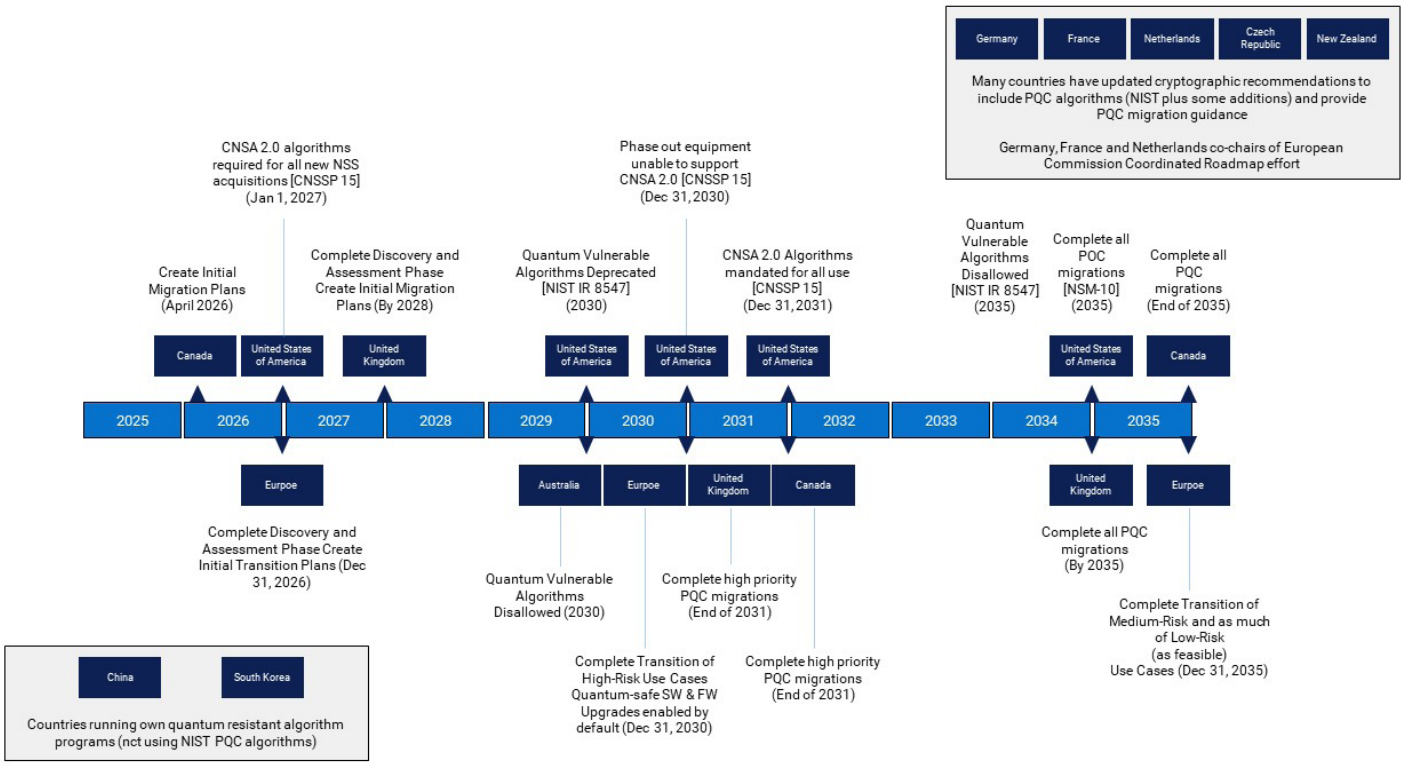
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

OMB Memorandum 23-02 (OMB M-23-02)
Provides detalied guidelines for federal agencies to how to comply with NSM-10

O CNSA 2.0, anunciado pela NSA em setembro de 2022, apresenta as primeiras recomendações para algoritmos criptográficos pós-quânticos. O CNSA 2.0 define prazos explícitos para a adoção de algoritmos resistentes à computação quântica em sistemas de segurança nacional (NSS) e serve como um guia avançado para as empresas prepararem suas próprias transições:



Outras organizações em todo o mundo também definiram diretrizes para a transição de PQC. Abaixo estão alguns dos diferentes mandatos de países.



Essas datas não são arbitrárias — elas refletem os prazos de entrega necessários para reprojetar, validar e implementar criptografia em ecossistemas complexos de TI. As empresas devem vê-los como mais do que mandatos governamentais; eles são indicadores práticos da mudança global em direção à resiliência quântica.

Colaboração do setor

Além do NIST e da NSA, a Dell está influenciando e participando ativamente de consórcios do setor e de grupos de padrões que estão impulsionando a interoperabilidade e a adoção. O Trusted Computing Group está integrando o PQC ao padrão Trusted Platform Module (TPM). O IETF, que vem impulsionando grande parte da integração dos algoritmos PQC em protocolos do setor, como TLS e certificados X.509, por exemplo. Os comitês OASIS Key Management Interoperability Protocol (KMIP) estão habilitando o PQC para estruturas de gerenciamento de chaves. A FIDO Alliance está estudando o impacto do PQC nos padrões de autenticação e integração de dispositivos, enquanto organizações como o SAFECode estão trabalhando para educar o setor sobre preparação para migração.

O National Cyber Security Center of Excellence (NCCoE) do NIST é a construção que permite que o NIST trabalhe com o setor, a academia e as agências governamentais por meio de projetos focados em domínio. Eles têm se concentrado em uma série de coisas, como:

- Descoberta criptográfica — identificando qual criptografia precisa ser migrada e como priorizar o que migrar primeiro.
- Interoperabilidade – garantindo que os recursos e protocolos criptográficos populares incorporem os novos algoritmos PQC e que a implementação seja interoperável entre diferentes fornecedores.
- Agilidade criptográfica: com foco no desenvolvimento de sistemas de informação que incentivam o suporte de rápidas adaptações de novos primitivos e algoritmos criptográficos sem fazer alterações significativas na infraestrutura do sistema, também conhecida como criptoagilidade

Esses projetos ajudam a informar/desenvolver orientações e padrões que eles criam e ajudam a garantir que existam exemplos de soluções do setor para os padrões e orientações que fornecem. A Dell participa do projeto do NCCoE de Migração para PQC desde seu surgimento.

Hoje, a PQC não é apenas um tópico de pesquisa; é um padrão em desenvolvimento com algoritmos concretos, cronogramas e caminhos de adoção. As organizações que começam a se preparar agora podem evitar o custo, a interrupção e o risco de uma corrida de última hora. A transição não se trata apenas de conformidade, mas de garantir que a confiança, a confidencialidade e a integridade permaneçam intactas à medida que a computação quântica remodela o cenário digital.

Por que o momento para agir é agora

O imediatismo da ameaça

Pode ser tentador ver a computação quântica como um risco distante, algo que pode ser resolvido quando a tecnologia estiver totalmente implementada. Na realidade, o relógio já foi iniciado. Informações confidenciais – transações financeiras, registros
de saúde, propriedade intelectual ou comunicações governamentais podem ser criptografados com segurança hoje, mas, uma vez que as máquinas quânticas atinjam o limite de quebrar RSA ou ECC, esses dados poderão ser expostos retroativamente. O resultado é que todo um backlog de comunicações e registros históricos pode repentinamente estar em risco.

Longos ciclos de tecnologia

Os ecossistemas modernos de TI não são transformados com facilidade ou rapidez. Historicamente, substituições de algoritmo individual, como a transição de SHA-1 para SHA-2 ou DES/3DES para AES, levaram mais de 10 anos para serem concluídas. Esses algoritmos estão profundamente incorporados em sistemas operacionais, aplicativos, dispositivos de rede e hardware. A substituição deles exige recriação, validação, teste e implementação em ambientes que abrangem desde data centers até plataformas de nuvem e dispositivos de borda. Para muitas organizações, isso levará anos, muito mais tempo do que o período restante antes que a computação quântica represente ameaças reais. É por isso que reguladores, órgãos de padronização e líderes de segurança enfatizam a preparação imediata. Esperar até que os CRQCs estejam amplamente disponíveis não deixará tempo para uma transição ordenada.

Riscos de falta de ação

As consequências do atraso na migração vão além da exposição técnica:

- Risco de segurança de dados: Dados de longa duração, como históricos médicos, registros financeiros ou informações de defesa, podem ser comprometidos retroativamente quando os computadores quânticos amadurecem.
- Risco de integridade e autenticidade do software: a autenticidade e a integridade do software podem ser comprometidas com código mal-intencionado se assinadas com os métodos de assinatura atuais e ainda em uso depois que os computadores quânticos amadurecerem.
- Risco operacional: Sistemas de infraestrutura crítica, como serviços públicos, redes de transporte e serviços de emergência, são notoriamente difíceis de atualizar. A falta de planejamento agora pode significar interrupção operacional mais tarde.
- Riscos regulatórios e de conformidade: Estruturas como **CNSA 2.0** estabeleceram prazos claros para a conformidade. Organizações que não se preparam correm o risco não apenas de exposição, mas também de não conformidade com as expectativas do governo ou da indústria.
- Riscos financeiros e de reputação: Uma violação resultante de vulnerabilidades criptográficas não abordadas pode levar a danos duradouros à confiança da marca, além de perdas financeiras significativas.

O caso da ação proativa

A preparação proativa não é meramente uma ação defensiva; é uma oportunidade para fortalecer a resiliência a longo prazo. Ao
realizar inventários criptográficos, atualizar comprimentos de chave simétricos, testar soluções prontas para PQC e interagir com fornecedores que disponibilizam ofertas com resistência quântica, as organizações podem garantir a continuidade da confiança. Os primeiros a adotar estão
mais bem posicionados para preparar operações futuras, manter a conformidade e demonstrar liderança para clientes, parceiros e órgãos reguladores.

A abordagem da Dell para criptografia pós-quântica

Na Dell, acreditamos que a tecnologia impulsiona o progresso humano, e a segurança é a base desse progresso. Como empresa, a Dell Technologies está garantindo que seu portfólio, infraestrutura de TI e sistemas de suporte do ciclo de vida estejam bem preparados para a transição para algoritmos resistentes à computação quântica. As medidas que estão sendo tomadas para se preparar para a transição incluem:

- Identificar as áreas e finalidades específicas em que a criptografia é empregada em produtos, serviços, infraestrutura de TI e sistemas de suporte para formular planos de transição abrangentes.
- Aprimorar o conhecimento interno sobre algoritmos de criptografia pós-quântica (PQC), considerando aspectos de implementação e princípios de projeto relacionados à agilidade criptográfica para facilitar uma transição tranquila para algoritmos PQC.
- Avaliar o desempenho, a aplicabilidade e a adequação dos algoritmos PQC em vários casos de uso relevantes para o diversificado portfólio da Dell Technologies.

Dada a complexidade da transição para PQC, os upgrades dos casos de uso criptográficos podem ser implementados gradualmente nas ofertas da Dell Technologies. Para exemplificar, do ponto de vista dos dados, a prioridade de transição é dada aos casos de uso que podem estar vulneráveis a ataques de "coletar agora, descriptografar depois", como criptografia de dados em trânsito ou em repouso.

Ao considerar sua plataforma de tecnologia, a transição de um caso de uso criptográfico pode envolver uma atualização/substituição completa do produto ou um upgrade do produto. Isso dependerá do produto em questão e de onde e como a criptografia é implementada nesse produto e nos sistemas adjacentes.

O lançamento de ofertas com resistência quântica será um foco nos próximos 5 anos para garantir que os clientes possam atender aos cronogramas de transição de PQC que serão publicados por governos e associações do setor entre 2027 e 2035.

Os clientes devem trabalhar com sua equipe de contas da Dell para obter detalhes específicos do produto (por exemplo, roteiros e cronogramas de lançamento) para incorporar em seus planos de migração. Convém prestar atenção, pois a Dell fornecerá cronogramas mais específicos para a integração de PQC em suas linhas de produtos e produtos nos próximos meses.

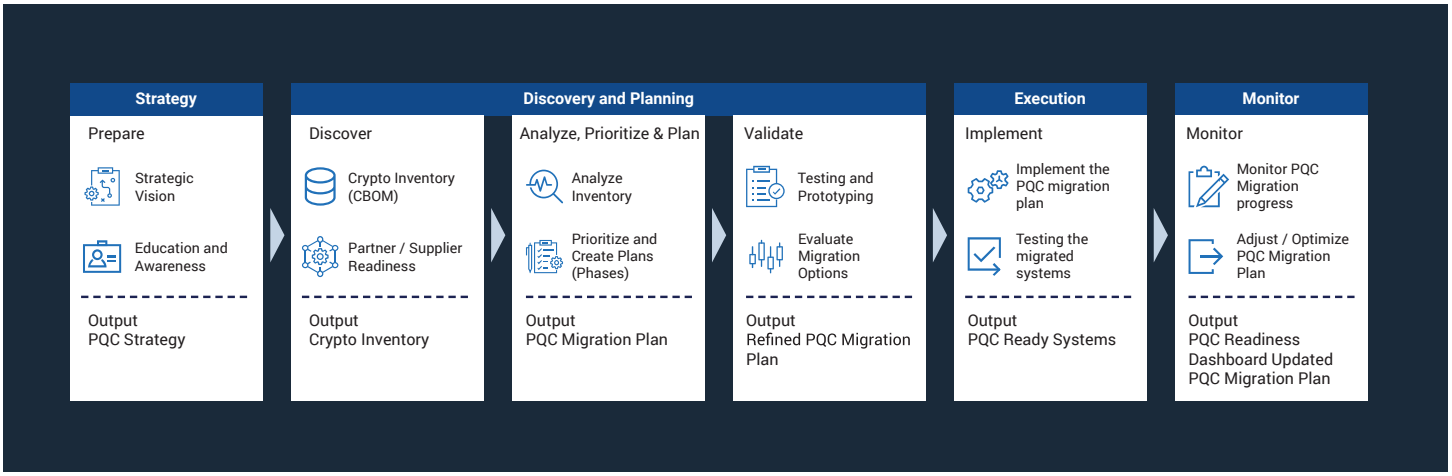
Preparação para a inovação em resiliência quântica

O objetivo da Dell não é apenas ajudar os clientes a cumprir os padrões emergentes, mas também capacitá-los a inovar com segurança na era quântica. Seja pela implementação de cargas de trabalho de IA, gerenciamento de ambientes de nuvem híbrida ou modernização da infraestrutura de borda, os clientes podem ter a confiança de que as soluções Dell são projetadas com resiliência em mente. A segurança não é adicionada depois — ela é projetada desde o início em todas as camadas do portfólio da Dell, garantindo que as organizações possam navegar na transição para a criptografia pós-quântica com confiança.

Preparação para a transição

A mudança para a criptografia pós-quântica será uma das mudanças de infraestrutura mais significativas em décadas. Essa transição afeta quase todos os aspectos de TI, desde servidores e armazenamento até endpoints, plataformas de nuvem e protocolos de rede. O sucesso requer previsão, planejamento e execução disciplinada. Na Dell Technologies, vemos que o caminho a seguir é uma jornada em fases: que equilibra melhorias imediatas de segurança com a prontidão em longo prazo para a adoção da PQC.

A Dell está preparada para ajudar você com sua estratégia de implementação de PQC. Recomendamos um plano de migração por fases e descrevemos um conjunto de atividades para ajudar você a criar estratégias, planejar, executar e monitorar sua migração para PQC.



Preparando a postura de segurança atual

Boa higiene da segurança

O primeiro passo para se preparar para o futuro quântico é reforçar as defesas já existentes. As organizações devem utilizar práticas recomendadas sólidas de higiene de segurança, como impor o acesso com privilégios mínimos, implementar a autenticação baseada em vários fatores e manter o gerenciamento rigoroso de patches. Também há duas outras considerações. Pode ser importante desativar a criptografia mais fraca para que novos sistemas com criptografia mais forte possam interoperar com sistemas legados. Também é importante que a criptografia simétrica, para sistemas mais recentes, seja atualizada para comprimentos de chave maiores, AES-256 e SHA-384 ou superior, para combater as margens reduzidas introduzidas pelo algoritmo de Grover. Essas medidas não apenas reduzem o risco de hoje, mas também minimizam o acúmulo de dívida criptográfica que, de outra forma, complicaria a migração de amanhã.

Inventário e auditoria de ativos criptográficos

A base de qualquer plano de migração é a visibilidade. As organizações devem realizar um inventário criptográfico abrangente, identificando onde e como a criptografia de chave pública é usada em aplicativos, dispositivos e fluxos de trabalho. Isso inclui certificados TLS, VPNs, sistemas de e-mail, mecanismos de assinatura de código e dados arquivados. Uma vez identificados, os ativos devem ser priorizados com base na importância, na sensibilidade e na vida útil dos negócios. Dados de longa duração, como registros médicos ou arquivos confidenciais, devem ser tratados com a máxima urgência, pois são os mais vulneráveis à ameaça de "coletar agora, descriptografar depois".

Piloto e experimento com a PQC

Assim que o cenário criptográfico for compreendido, as organizações devem começar a testar soluções de PQC em ambientes controlados. Ao testar essas soluções em laboratórios, as equipes de TI podem validar o desempenho, a interoperabilidade e a capacidade de gerenciamento antes da implementação em larga escala. Criando agilidade criptográfica - a capacidade de alternar algoritmos criptográficos sem reformular sistemas inteiros, é fundamental para a resiliência a longo prazo e a facilidade de migração.

Adote uma abordagem de interoperabilidade

À medida que os padrões amadurecem, um modelo híbrido fornece uma ponte para o futuro. Muitos fornecedores já estão oferecendo suporte a cipher suites híbridos que combinam algoritmos clássicos e resistentes à computação quântica em uma única implementação. Essa abordagem dupla proporciona continuidade de proteção, mesmo que um algoritmo seja comprometido posteriormente. As empresas devem começar a adotar estratégias híbridas agora, alinhando seus cronogramas internos com marcos e roteiros do produto de seu fornecedor de infraestrutura. Isso garante que, à medida que os algoritmos resistentes à computação quântica atingem a padronização, as organizações possam escalar a adoção sem interrupções.

Execute a migração completa e a validação contínua

O objetivo final é uma transição completa para PQC em toda a empresa. Isso não será um evento isolado, mas um processo contínuo de validação e adaptação. As organizações devem executar planos detalhados de migração, incorporando a PQC em todas as camadas de sua pilha de TI, enquanto testam continuamente novos padrões e implementações. Usando laboratórios híbridos quântico-clássicos, os clientes podem simular cenários de ataque, validar a integridade criptográfica e garantir que seus sistemas permaneçam resilientes contra ameaças em evolução.

Colaboração e compartilhamento de conhecimento

Por fim, nenhuma organização deve enfrentar esse desafio sozinha. Os consórcios do setor, pesquisadores acadêmicos e agências governamentais estão reunindo conhecimento para acelerar a transição para PQC. A participação em grupos de padronização, grupos de trabalho e programas piloto permite que as empresas se mantenham alinhadas com as melhores práticas e os requisitos emergentes. O envolvimento ativo da Dell em iniciativas como o projeto PQC do NCCoE da NIST garante que nossos clientes se beneficiem diretamente dessa experiência coletiva.

A preparação para a PQC é uma maratona, não uma corrida. Ao adotar uma abordagem por fases, reforçando as defesas atuais, auditando ativos criptográficos, testando PQC, adotando estratégias híbridas e executando uma migração completa, as organizações podem avançar com confiança em direção à resiliência quântica. Com a Dell como parceira, essa jornada não é apenas viável, mas também uma oportunidade para fortalecer a confiança e viabilizar a inovação no futuro.

Aplicações no mundo real e benefícios

A transição para a criptografia pós-quântica é mais do que um exercício de conformidade; é um imperativo comercial que impacta diretamente a confiança, a resiliência e a competitividade a longo prazo. Para provedores de telecomunicações, instituições financeiras, organizações de saúde e agências governamentais, a adoção de algoritmos resistentes à computação quântica garante que a infraestrutura digital crítica permaneça segura contra ameaças atuais e futuras.

Telecomunicações

As redes de telecomunicações são o backbone da digitalização global. Elas viabilizam tudo, desde serviços de emergência e conectividade da IoT até comunicações seguras com o cliente. Uma violação quântica nesse setor poderia comprometer o provisionamento de SIM, a integração de eSIM ou os processos de autenticação que sustentam o 4G e o 5G. Ao implementar criptografia híbrida e resistente à computação quântica agora, os operadores podem manter a confiança do cliente, proteger a privacidade dos dados e garantir a continuidade perfeita do serviço em todas as gerações de tecnologia móvel.

Serviços financeiros

O setor financeiro está entre os mais visados por adversários cibernéticos, e a integridade das transações depende da criptografia. A prontidão pós-quântica protege pagamentos digitais, serviços bancários on-line e transferências interbancárias contra fraudes habilitadas para criptografia quântica. A adoção precoce também tranquiliza reguladores e clientes, demonstrando que as instituições estão comprometidas com a proteção de ativos e a manutenção da estabilidade sistêmica. A criptografia preparada para o futuro nesse setor reduz tanto a exposição regulatória quanto o risco à reputação.

Área da saúde

Registros de pacientes, dados genômicos e dispositivos médicos conectados estão todos em risco de ataques do tipo "coletar agora, descriptografar depois". O setor de saúde enfrenta um desafio adicional: os longos períodos de retenção exigidos para dados médicos confidenciais. Ao iniciar a transição para a PQC hoje, hospitais e provedores garantem que os registros de saúde permaneçam privados não apenas agora, mas também nas próximas décadas. Isso é essencial para preservar a confiança do paciente e, ao mesmo tempo, atender às regulamentações de proteção de dados em evolução.

Infraestrutura crítica e governamental

De comunicações de defesa a sistemas de distribuição de energia, governos e operadores de infraestrutura dependem da criptografia para a continuidade das operações e a segurança nacional. A criptografia pós-quântica protege não apenas contra adversários de curto prazo, mas também contra a coleta estratégica de comunicações criptografadas para exploração futura. O alinhamento com estruturas como CNSA 2.0 garante que os sistemas governamentais permaneçam interoperáveis, seguros e confiáveis na era quântica.

Benefícios comerciais mais amplos

Embora a necessidade técnica da PQC seja clara, o caso de negócios é igualmente forte:

- Confiança e reputação da marca: Demonstra liderança na proteção de dados de clientes e parceiros.
- Conformidade normativa: Alinha-se aos padrões NIST e às exigências governamentais, como CNSA 2.0.
- Resiliência operacional: Reduz o risco de interrupções catastróficas causadas por falhas na criptografia.
- Diferenciação competitiva: Posiciona as organizações como inovadoras proativas em vez de seguidoras reativas.

Os benefícios de agir agora vão muito além da resiliência técnica. As organizações que adotarem a PQC desde o início não apenas reduzirão os riscos, mas também fortalecerão sua capacidade de inovar, cumprir as normas e competir em uma economia digital que depende da confiança.

Dê os próximos passos

A chegada da computação quântica representa tanto uma oportunidade geracional quanto um desafio de segurança sem precedentes. Embora o cronograma exato para computadores quânticos relevantes para a criptografia permaneça incerto, o que é certo é o esforço necessário para se preparar. A transição para a criptografia pós-quântica exigirá anos de planejamento, investimento e execução coordenados. Não é uma opção viável esperar até que os computadores quânticos estejam operacionais.

O primeiro passo para qualquer organização é a conscientização: entender onde e como a criptografia é usada em seu ambiente. A partir daí, as empresas devem iniciar o processo de inventário, priorização e teste de soluções seguras contra a computação quântica. A criptografia híbrida, que combina algoritmos clássicos e pós-quânticos, oferece um caminho imediato para a resiliência, enquanto os padrões continuam a evoluir. Ao alinhar roteiros internos com estruturas globais, como os padrões de PQC do NIST e os cronogramas do CNSA 2.0, as organizações podem avançar com confiança em direção à conformidade e à interoperabilidade.

A Dell Technologies está comprometida em ajudar os clientes a navegar nessa transição. Por meio de nossa abordagem, fornecemos uma base de integridade da cadeia de suprimentos, proteções incorporadas ao hardware e adaptabilidade habilitada por software. Nossas parcerias com os principais provedores de segurança e nossa participação ativa em órgãos de padronização do setor garantem que as soluções da Dell não estejam apenas alinhadas com os requisitos mais recentes, mas também sejam testadas quanto ao desempenho e à interoperabilidade no mundo real.

Comece a se preparar hoje mesmo. Comece com a descoberta e a análise de riscos, envolva-se com fornecedores confiáveis e teste tecnologias resistentes à computação quântica. Cada passo dado agora reduz o risco de interrupção amanhã. As organizações que agirem com antecedência não apenas protegerão seus dados e sistemas, mas também conquistarão a confiança de clientes, reguladores e parceiros em uma era em que a confiança digital é fundamental.

Sobre nossa empresa

A Dell Technologies tem o compromisso de tornar a tecnologia avançada acessível, confiável e habilitada para todos. Ajudamos pessoas e organizações a aproveitar a inovação com segurança, abrindo caminho para um futuro mais seguro, inclusivo e conectado.