DELL Technologies

Documento técnico

Criptografía poscuántica: preparación para la era cuántica

Documento técnico de Dell Technologies

Índice

Resumen ejecutivo

La computación cuántica está pasando rápidamente de la investigación teórica a la realidad práctica. Antes se consideraba un horizonte distante, pero los avances en hardware, algoritmos e inversión están acelerando la llegada de máquinas capaces de resolver problemas que los ordenadores clásicos no pueden. Las implicaciones para la industria son profundas. La computación cuántica promete desbloquear una innovación que antes estaba fuera de nuestro alcance, ya se trate del descubrimiento de medicamentos, el modelado del clima o la logística global.

Sin embargo, este avance conlleva un reto disruptivo: los ordenadores cuánticos socavarán los cimientos criptográficos que protegen la economía digital. La criptografía de clave pública (algoritmos como RSA y la criptografía de curva elíptica [ECC]) lleva décadas protegiendo las comunicaciones digitales, los sistemas financieros, los historiales de los servicios de salud y la seguridad nacional. Estos métodos se basan en problemas matemáticos que los ordenadores clásicos no pueden resolver. Sin embargo, con la llegada de los ordenadores cuánticos criptográficamente relevantes (CRQC), estos mismos problemas se pueden resolver de manera eficiente, lo que hace que la seguridad actual quede obsoleta.

Esta amenaza no es teórica. Algunas organizaciones ya están utilizando una táctica conocida como "cosechar ahora, descifrar después" (HNDL), que consiste en recopilar datos cifrados hoy con la expectativa de desglosarlos una vez que los ordenadores cuánticos maduren. La información confidencial que parece segura ahora puede ser vulnerable en cuestión de años. El momento de actuar no es cuando lleguen los CRQC, sino hoy.

En este documento técnico se explica la urgencia de la amenaza cuántica, se explora el campo emergente de la criptografía poscuántica (PQC) y se ofrece orientación acerca de cómo pueden prepararse las organizaciones. En él, se destaca el compromiso de Dell Technologies con la creación de un futuro cuántico seguro, que integre la seguridad en nuestra cadena de suministro, hardware, firmware, software y ecosistema de socios, alineándose con los estándares de criptografía poscuántica (PQC) del NIST (FIPS 203, FIPS 204 y FIPS 205) y con las directrices de Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). El objetivo de Dell es claro: garantizar que la innovación pueda avanzar sin sacrificar la seguridad ni la confianza.

Terminología

A lo largo de este documento, encontrará una serie de términos. Hemos intentado explicar a grandes rasgos algunos de estos términos para ayudar a comprender el documento.

Criptografía poscuántica: un nuevo enfoque matemático de la criptografía, con nuevos algoritmos, diseñados para proteger frente a ataques de ordenadores cuánticos. Estos algoritmos se ejecutan en ordenadores clásicos y son resistentes tanto a los ataques cuánticos como a los conocidos ataques criptográficos clásicos.

Resiliencia cuántica: la resiliencia cuántica hace referencia a sistemas, algoritmos o infraestructuras diseñados para que sigan siendo seguros incluso en presencia de ordenadores cuánticos criptográficamente relevantes (CRQC). Un sistema con resiliencia cuántica utiliza criptografía poscuántica (PQC) u otras protecciones que resisten los ataques clásicos y cuánticos, lo que garantiza la confidencialidad, integridad y autenticidad de los datos en el futuro. Otros términos, como resiliencia cuántica y seguridad cuántica, también se utilizan indistintamente.

Agilidad criptográfica (a veces denominada criptoagilidad): es la capacidad de los sistemas y las aplicaciones de una organización para cambiar de forma rápida y optimizada algoritmos criptográficos, protocolos o longitudes de clave sin necesidad de rediseños importantes ni interrupciones operativas.

"Cosechar ahora, descifrar después" (HNDL): también se conoce como "registrar ahora, descifrar después" y es el acto de que los adversarios recopilen y almacenen datos cifrados hoy con la intención de descifrarlos en el futuro una vez que los ordenadores cuánticos criptográficamente relevantes (CRQC) estén disponibles.

Computación cuántica y la amenaza para el cifrado

El auge de la computación cuántica

Como describimos hace casi un año en la entrada de blog Criptografía poscuántica: un imperativo estratégico para la resiliencia empresarial de nuestro director de tecnología John Roese, los ordenadores clásicos, ya sean portátiles, teléfonos inteligentes o servidores, procesan la información utilizando bits, que existen en un estado de cero o uno. Este modelo binario ha impulsado décadas de progreso, pero limita la forma en que se puede representar y manipular la información. Los ordenadores cuánticos utilizan cúbits, que pueden existir en varios estados simultáneamente a través de principios como la superposición y el entrelazamiento. Esto permite a las máquinas cuánticas explorar grandes cantidades de posibles soluciones en paralelo, lo que ofrece una ventaja computacional para clases específicas de problemas.

Las posibles aplicaciones de la computación cuántica son extraordinarias. Los investigadores prevén avances en el sector farmacéutico mediante la simulación de las interacciones moleculares con una precisión que los ordenadores clásicos no pueden lograr. Los científicos del clima visualizan modelos más precisos de sistemas globales, mientras que el sector energético ve potencial para optimizar las redes eléctricas y el almacenamiento de energía. Incluso la logística y la fabricación se beneficiarán de las técnicas de optimización cuántica. Los beneficios son reales y están a nuestro alcance, pero también los riesgos.

Por qué el cifrado está en riesgo

El cifrado sustenta la confianza en la era digital. Cuando introduce un número de tarjeta de crédito, inicia sesión en un sitio web seguro o recibe una actualización de software firmada, la criptografía garantiza la confidencialidad, la autenticidad y la integridad. La mayor parte de esta protección se basa en criptografía de clave pública, algoritmos como RSA y ECC que se basan en problemas matemáticos considerados computacionalmente inviables para las máquinas clásicas.

La computación cuántica cambia esta ecuación. Utilizando el **algoritmo de Shor**, un ordenador cuántico suficientemente potente puede resolver los problemas de factorización y logaritmo discreto que aportan su resistencia a RSA y ECC. Una vez que existan los CRQC, las firmas digitales que protegen las actualizaciones de software, las claves que establecen las sesiones de TLS y los certificados que autentican los dispositivos pueden verse en riesgo. El impacto es sistémico y amenaza los mecanismos que hacen que las transacciones digitales sean seguras.

La criptografía simétrica (algoritmos como AES utilizados para proteger los datos almacenados o las comunicaciones seguras) se enfrenta a un desafío diferente, aunque menos grave. El **algoritmo de Grover** permite que un ordenador cuántico reduzca la resistencia efectiva de las claves simétricas, lo que reduce a la mitad su seguridad. Aunque esto puede mitigarse cambiando a tamaños de clave más grandes, como AES-256, el ajuste subraya el alcance generalizado de las amenazas cuánticas.

Urgencia y consecuencias

Las consecuencias van mucho más allá del riesgo teórico. Las organizaciones que no se preparen se enfrentan a exposición de la propiedad intelectual confidencial, interrupción de los sistemas financieros, filtraciones de los datos de los servicios de salud y amenazas a la seguridad nacional. La estrategia "cosechar ahora, descifrar después" agrava la urgencia: los adversarios solo necesitan capturar datos cifrados hoy y esperar a que se disponga de los medios para descifrarlos. Cuando lleguen los CRQC, los daños ya serán irreversibles.

Criptografía poscuántica y estándares emergentes

Definición de la criptografía poscuántica

La criptografía poscuántica (PQC) hace referencia a una nueva generación de algoritmos diseñados para proteger los sistemas digitales frente a ataques clásicos y cuánticos. A diferencia de la distribución cuántica de claves, que requiere hardware especializado, la PQC se ha diseñado para ejecutarse en la infraestructura clásica actual (servidores, puntos finales y redes), por lo que es la forma más práctica y ampliable de prepararse para la era cuántica.

La base de la PQC es un conjunto de problemas matemáticos que, según los conocimientos actuales, son resistentes a técnicas cuánticas como los algoritmos de Shor y Grover. La criptografía basada en entramados, las firmas basadas en hash, los esquemas basados en código y las ecuaciones multivariables representan las familias más prometedoras. Estos enfoques se están probando y estandarizando rigurosamente para garantizar que proporcionen la misma fiabilidad e interoperabilidad que RSA y ECC una vez distribuidos.

El esfuerzo de estandarización global: estándares emergentes del sector

Reconociendo la urgencia de la amenaza, los gobiernos y los organismos de normalización han convertido la PQC en una prioridad mundial. El Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. lanzó su proyecto de PQC en 2016, pidiendo a la comunidad de investigación criptográfica que proponga, analice y perfeccione los algoritmos candidatos. Después de años de pruebas, el NIST anunció el primer grupo de algoritmos estandarizados en agosto de 2024:

- **CRYSTALS**-Kyber para el cifrado de claves públicas y el establecimiento de claves
- **CRYSTALS**-Dilithium y SPHINCS+ para las firmas digitales

Aún se están revisando algoritmos adicionales para ofrecer diversidad y flexibilidad para las diferentes necesidades de implementación, incluidos sistemas ligeros como el firmware incorporado. Este proceso de estandarización en evolución garantiza que las organizaciones de todo el mundo tengan un camino claro para adoptar soluciones resistentes a la computación cuántica.

Estándares del NIST: FIPS 203, 204 y 205

En agosto de 2024, el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. finalizó los primeros algoritmos de PQC:

- FIPS 203 (ML-KEM): basado en CRYSTALS-Kyber, es un mecanismo de encapsulación de claves. Proporciona seguridad IND-CCA2, lo que significa que los textos cifrados siguen siendo indistinguibles incluso bajo ataques de texto cifrado elegido adaptativo.
- FIPS 204 (ML-DSA): basado en CRYSTALS-Dilithium, es un algoritmo de firmas digitales. Ofrece una sólida seguridad EUF-CMA (incapacidad de falsificación existencial en ataques de mensaje elegido), el requisito estándar para las firmas digitales.
- FIPS 205 (SLH-DSA): basado en SPHINCS+, es un esquema de firmas basado en hash. Se ha seleccionado como una alternativa conservadora que no depende de problemas de entramado.

Un roadmap obligatorio

Conscientes de la importancia de adoptar algoritmos de cifrado resistentes a la computación cuántica, el gobierno federal de EE. UU. ha comenzado a enviar requisitos de PQC a las agencias federales. Entre ellos se incluyen 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 y Office of Management and Budget Memorandum 23-02 (OMB M-2302), entre otros.

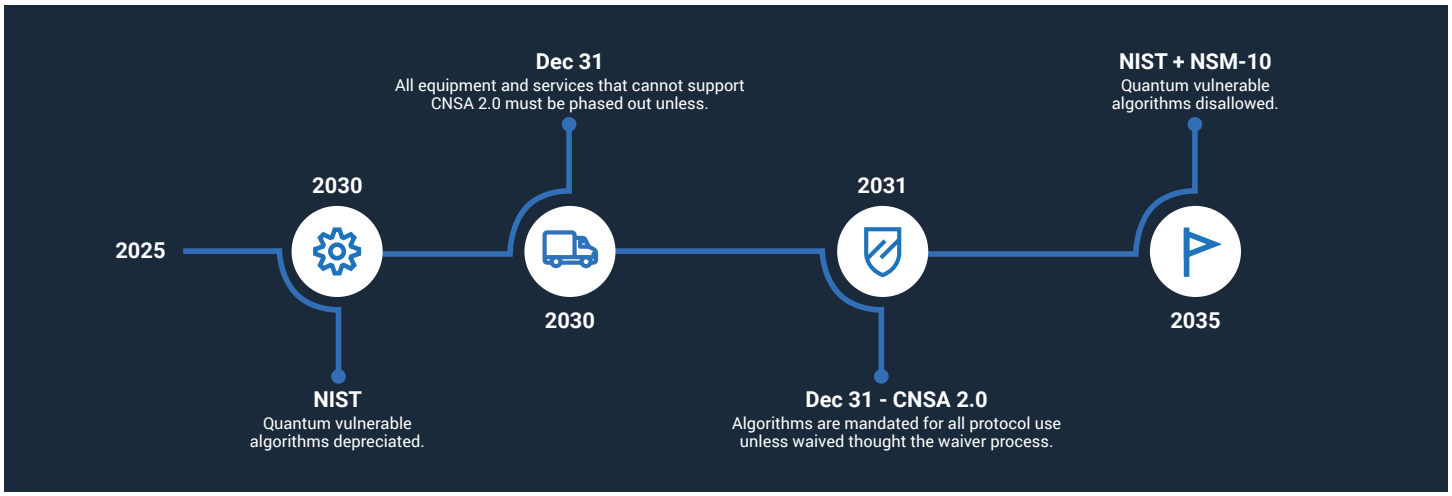
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodogies.

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

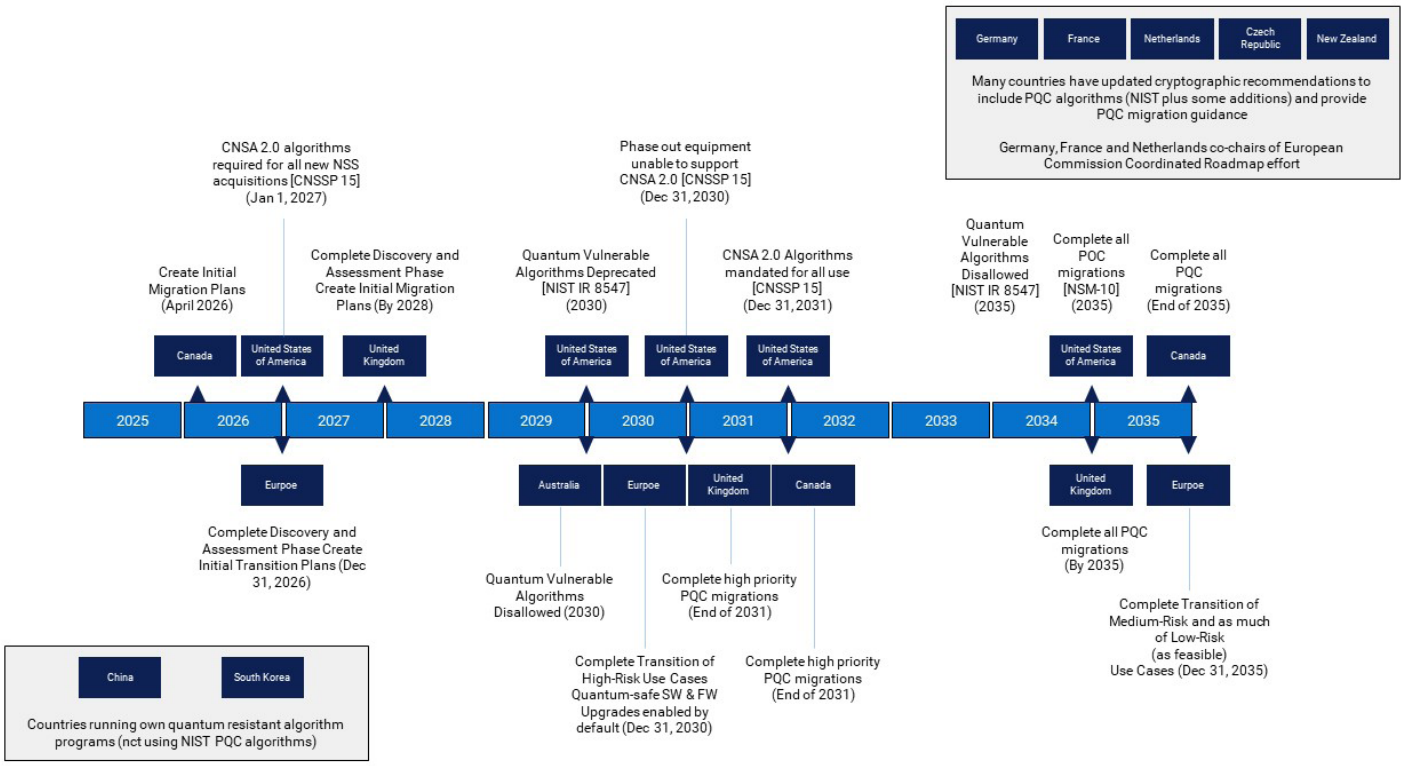
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

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

CNSA 2.0, anunciado por la NSA en septiembre de 2022, presenta las primeras recomendaciones para los algoritmos criptográficos poscuánticos. CNSA 2.0 establece plazos explícitos para la adopción de algoritmos resistentes a la computación cuántica en los sistemas nacionales de seguridad (NSS), y sirve como una potente guía para las empresas que están preparando sus propias transiciones:



Otras organizaciones de todo el mundo también han establecido directrices para la transición a la PQC. A continuación se indican algunos de los mandatos de los distintos países.



Estas fechas no son arbitrarias: reflejan los plazos de entrega necesarios para rediseñar, validar e implementar la criptografía en ecosistemas de TI complejos. Las empresas deben considerarlos más que mandatos gubernamentales; son indicadores prácticos del cambio mundial hacia la resiliencia cuántica.

Colaboración en el sector

Más allá del NIST y la NSA, Dell está influyendo y participando activamente en consorcios del sector y grupos normalización que impulsan la interoperabilidad y la adopción. Trusted Computing Group está integrando la PQC en el estándar Trusted Platform Module (TPM). El IETF está impulsando gran parte de la integración de los algoritmos de PQC en protocolos del sector, como TLS y certificados X.509, por ejemplo. Los comités del protocolo de interoperabilidad de administración de claves (KMIP) de OASIS están habilitando la PQC para las infraestructuras de gestión de claves. FIDO Alliance está estudiando el impacto de la PQC en los estándares de autenticación e incorporación de dispositivos, mientras que organizaciones como SAFECode trabajan para educar al sector sobre la preparación para la migración.

El National Cyber Security Center of Excellence del NIST (NCCoE) es el constructo que permite al NIST trabajar con la industria, el mundo académico y las agencias gubernamentales a través de proyectos centrados en dominios. Se han centrado en una serie de aspectos como:

- Descubrimiento criptográfico: identifica qué criptografía es necesario migrar y cómo priorizar qué migrar primero.
- Interoperabilidad: garantizar que las funciones y protocolos criptográficos más populares incorporen los nuevos algoritmos de PQC y que la implementación de diferentes proveedores interopere.
- Criptoagilidad: se centra en desarrollar sistemas de información que fomenten la compatibilidad con adaptaciones rápidas de los nuevos primitivos y algoritmos criptográficos sin realizar cambios significativos en la infraestructura del sistema, lo que también se conoce como agilidad criptográfica.

Estos proyectos ayudan a fundamentar y desarrollar la orientación y los estándares que crean y ayudan a garantizar que existan soluciones de ejemplo del sector para los estándares y la orientación que proporcionan. Dell ha participado en el proyecto de migración a la PQC del NCCoE desde su concepción.

Actualmente, la PQC no es solo un tema de investigación; es un estándar en desarrollo con algoritmos, plazos y rutas de adopción concretos. Las organizaciones que empiecen a prepararse ahora pueden evitar los costes, las interrupciones y el riesgo de una desbandada de última hora. La transición no se basa simplemente en el cumplimiento normativo: se trata de garantizar que la confianza, la confidencialidad y la integridad permanezcan intactas a medida que la computación cuántica remodele el panorama digital.

Por qué es el momento de actuar

La inmediatez de la amenaza

Puede ser tentador ver la computación cuántica como un riesgo distante, algo que se puede abordar una vez que la tecnología se haya materializado plenamente. En realidad, el reloj ya está en marcha. La información confidencial (transacciones financieras, historiales de los servicios de salud, propiedad intelectual o comunicaciones gubernamentales) puede cifrarse de forma segura en la actualidad, pero una vez que las máquinas cuánticas alcancen el umbral de descomponer RSA o ECC, esos datos pueden verse expuestos retroactivamente. El resultado es que, de repente, todo una acumulación de comunicaciones y registros históricos podría estar en riesgo.

Ciclos tecnológicos largos

Los ecosistemas de TI modernos no se transforman fácil o rápidamente. Históricamente, las sustituciones de algoritmos únicos, como la transición de SHA-1 a SHA-2 o de DES/3DES a AES, han tardado más de 10 años en completarse. Estos algoritmos están profundamente integrados en los sistemas operativos, las aplicaciones, los dispositivos de red y el hardware. Su sustitución requiere rediseño, validación, pruebas e implementación en entornos que van desde centros de datos hasta plataformas de cloud y dispositivos perimetrales. En muchas organizaciones, esto tardará años, mucho más que el plazo restante antes de que la computación cuántica plantee amenazas para el mundo real. Por este motivo, los reguladores, los organismos de normalización y los líderes de seguridad hacen hincapié en la preparación inmediata. Esperar a que los CRQC estén ampliamente disponibles no dejará tiempo para una transición ordenada.

Riesgos de inacción

Las consecuencias de retrasar la migración van más allá de la exposición técnica:

- Riesgo de seguridad de los datos: los datos longevos, como los historiales médicos, los registros financieros o la información de defensa, pueden verse en riesgo retroactivamente una vez que los ordenadores cuánticos maduren.
- Riesgo de autenticidad e integridad del software: la autenticidad y la integridad del software pueden verse en riesgo con código malicioso si se firma con los métodos de firma actuales y se sigue utilizando una vez que los ordenadores cuánticos maduren.
- Riesgo operativo: los sistemas de infraestructura crítica (como los servicios públicos, las redes de transporte y los servicios de emergencia) son bastante difíciles de actualizar. Si no se planifica ahora, podría producirse una interrupción operativa más adelante.
- Riesgo normativo y de cumplimiento: marcos como **CNSA 2.0** han establecido plazos claros para el cumplimiento normativo. Las organizaciones que no se preparen se enfrentarán al riesgo no solo de exposición, sino también de incumplimiento de las expectativas gubernamentales o del sector.
- Riesgo financiero y para la reputación: una filtración resultante de vulnerabilidades criptográficas no abordadas podría provocar daños duraderos en la confianza de la marca, junto con pérdidas financieras importantes.

El caso de la acción proactiva

La preparación proactiva no es simplemente una medida defensiva, sino una oportunidad para fortalecer la resiliencia a largo plazo. Mediante la realización de inventarios criptográficos, la actualización de las longitudes de claves simétricas, la realización de pruebas de soluciones preparadas para la PQC y la colaboración con proveedores que ofrezcan soluciones resistentes a la computación cuántica, las organizaciones pueden garantizar la continuidad de la confianza. Los primeros usuarios están mejor posicionados para las operaciones preparadas para el futuro, mantener el cumplimiento normativo y demostrar el liderazgo a clientes, socios y reguladores.

Enfoque de Dell sobre la criptografía poscuántica

En Dell, creemos que la tecnología impulsa el progreso humano y la seguridad es la base de ese progreso. Como empresa, Dell Technologies se está asegurando de que su cartera, su infraestructura de TI y sus sistemas de asistencia durante el ciclo de vida estén bien preparados para la transición a algoritmos resistentes a la computación cuántica. Entre las medidas que se están adoptando para prepararse para la transición se incluyen las siguientes:

- Identificar las áreas y los fines específicos en los que se emplea la criptografía en productos, servicios, infraestructuras de TI y sistemas de asistencia para formular planes de transición integrales.
- Mejorar el conocimiento interno sobre los algoritmos de criptografía poscuántica (PQC), teniendo en cuenta los aspectos de implementación y los principios de diseño relacionados con la criptoagilidad para facilitar una transición fluida a los algoritmos de PQC.
- Evaluar el rendimiento, la aplicabilidad y la idoneidad de los algoritmos de PQC en varios casos de uso relevantes para la cartera diversa de Dell Technologies.

Dada la compleja naturaleza de la transición a la PQC, las actualizaciones de los casos de uso criptográficos pueden incorporarse gradualmente a las ofertas de Dell Technologies. A modo de ejemplo, desde el punto de vista de los datos, se da prioridad a la transición a los casos de uso que podrían ser vulnerables a ataques de tipo "cosechar ahora, descifrar después", como el cifrado de datos en transferencia o en reposo.

Al considerar su plataforma tecnológica, la transición de un caso de uso criptográfico podría implicar una renovación o sustitución de todos los productos o una actualización de estos. Esto dependerá del producto en cuestión y de dónde y cómo se implemente la criptografía en ese producto y en los sistemas circundantes.

El lanzamiento de ofertas resistentes a la computación cuántica será un objetivo central en los próximos 5 años para garantizar que los clientes puedan cumplir los plazos de transición a la PQC que publiquen los gobiernos y las asociaciones del sector entre 2027 y 2035.

Los clientes deben colaborar con su equipo de cuentas de Dell para obtener detalles específicos de los productos (por ejemplo, roadmaps y plazos) para incorporarlos a sus planes de migración. Manténgase atento, ya que Dell ofrecerá plazos más específicos para la integración de la PQC en sus gamas de productos y productos en los próximos meses.

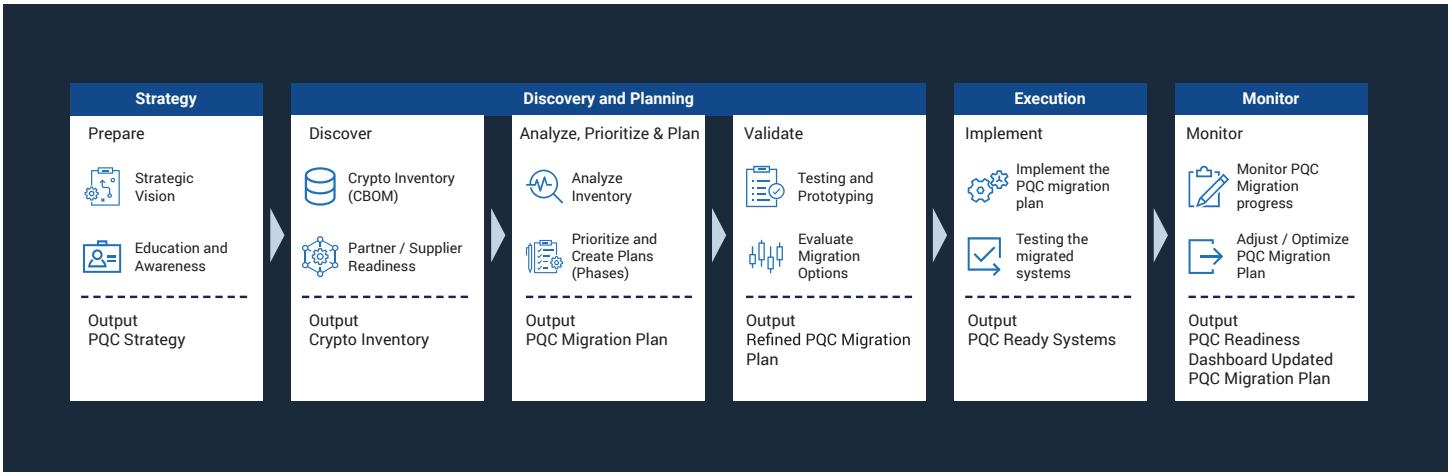
Preparación para la innovación con resiliencia cuántica

El objetivo de Dell no solo es ayudar a los clientes a cumplir con los estándares emergentes, sino también capacitarlos para innovar de forma segura en la era cuántica. Ya se trate de implementar cargas de trabajo de IA, gestionar entornos de cloud híbrida o modernizar la infraestructura perimetral, los clientes pueden confiar en que las soluciones de Dell se han diseñado pensando en la resiliencia. La seguridad no se integra después del diseño, se diseña en cada capa de la cartera de Dell, garantizando que las organizaciones pueden gestionar la transición a la criptografía poscuántica con confianza.

Preparación para la transición

El cambio a la criptografía poscuántica será uno de los cambios de infraestructura más significativos en décadas. Esta transición afecta a casi todos los aspectos de la TI, desde servidores y almacenamiento hasta puntos finales, plataformas de cloud y protocolos de red. El éxito requiere previsión, planificación y una ejecución disciplinada. En Dell Technologies, vemos el camino a seguir como un proceso por fases que equilibre las mejoras de seguridad inmediatas con la preparación a largo plazo para la adopción de la PQC.

En Dell estamos preparados para ayudarle con su estrategia para implementar la PQC. Recomendamos un plan de migración por fases y hemos resumido un conjunto de actividades para ayudarle a diseñar estrategias, planificar, ejecutar y supervisar la migración a la PQC.



Preparación del estado de seguridad actual

Buena higiene de seguridad

El primer paso para prepararse para el futuro cuántico es reforzar las defensas ya existentes. Las organizaciones deben utilizar prácticas recomendadas de higiene de seguridad sólidas, como imponer el acceso con privilegios mínimos, implementar la autenticación multifactor y mantener una rigurosa gestión de parches. También hay otras dos consideraciones. Puede ser importante deshabilitar una criptografía más débil, de modo que los sistemas nuevos con criptografía más alta puedan interoperar con los sistemas heredados. También es importante que la criptografía simétrica, para los sistemas más nuevos, se actualice a longitudes de clave más largas (AES-256 y SHA-384 o superiores) para contrarrestar los márgenes reducidos introducidos por el algoritmo de Grover. Estas medidas no solo reducen el riesgo hoy, sino que también minimizan la acumulación de la deuda criptográfica que, de lo contrario, complicaría la migración en el futuro.

Inventario y auditoría de activos criptográficos

La piedra angular de cualquier plan de migración es la visibilidad. Las organizaciones deben llevar a cabo un inventario criptográfico completo que identifique dónde y cómo se utiliza la criptografía de clave pública en aplicaciones, dispositivos y flujos de trabajo. Esto incluye certificados TLS, VPN, sistemas de correo electrónico, mecanismos de firma de código y datos archivados. Una vez identificados, los activos deben priorizarse en función de la importancia empresarial, la confidencialidad y la vida útil. Los datos longevos, como las historias clínicas o los archivos clasificados, deben tratarse con la máxima urgencia, ya que son más vulnerables a la amenaza de "cosechar ahora, descifrar después".

Pruebas piloto y experimentación con la PQC

Una vez que se conozca el panorama criptográfico, las organizaciones deben comenzar a probar soluciones de PQC en entornos controlados. Mediante pruebas piloto de estas soluciones en laboratorios, los equipos de TI pueden validar el rendimiento, la interoperabilidad y la capacidad de gestión antes de la implementación a gran escala. Desarrollar esta criptoagilidad (la capacidad de cambiar algoritmos criptográficos sin revisar sistemas enteros) es fundamental para la resiliencia a largo plazo y la facilidad de migración.

Adopción de un enfoque de interoperabilidad

A medida que los estándares maduran, un modelo híbrido proporciona un puente hacia el futuro. Muchos proveedores ya admiten conjuntos de cifrado híbridos que combinan algoritmos clásicos y resistentes a la computación cuántica en una sola implementación. Este doble enfoque proporciona continuidad de la protección incluso si un algoritmo se ve en riesgo más adelante. Las empresas deben empezar a adoptar estrategias híbridas ahora, al tiempo que alinean sus plazos internos con los roadmaps de productos y los hitos de su proveedor de infraestructura. Esto garantiza que, a medida que los algoritmos con seguridad cuántica alcancen la estandarización, las organizaciones puedan ampliar la adopción sin interrupciones.

Ejecución de la migración completa y validación continua

El objetivo final es una transición completa a la PQC en toda la empresa. No se tratará de un evento puntual, sino de un proceso continuo de validación y adaptación. Las organizaciones deben ejecutar planes de migración detallados, incorporando la PQC en todas las capas de su pila de TI y, al mismo tiempo, probar continuamente nuevos estándares e implementaciones. Mediante laboratorios híbridos de computación clásica y cuántica, los clientes pueden simular escenarios de ataque, validar la integridad criptográfica y garantizar que sus sistemas sigan siendo resilientes frente a las amenazas en constante evolución.

Colaboración e intercambio de conocimientos

Por último, ninguna organización debe afrontar este desafío por sí sola. Los consorcios del sector, los investigadores académicos y las agencias gubernamentales comparten conocimientos para acelerar la transición a la PQC. La participación en grupos de estándares, grupos de trabajo y programas piloto permite a las empresas mantenerse alineadas con las prácticas recomendadas y los requisitos emergentes. La participación activa de Dell en iniciativas como el proyecto de PQC del NCCoE del NIST garantiza que nuestros clientes se beneficien directamente de estos conocimientos colectivos.

La preparación para la PQC es un maratón, no un sprint. Mediante la adopción de un enfoque por fases (reforzar las defensas actuales, auditar los activos criptográficos, realizar pruebas piloto de PQC, adoptar estrategias híbridas y ejecutar una migración completa), las organizaciones pueden avanzar con confianza hacia la resiliencia cuántica. Con Dell como socio, este proceso no solo es posible, sino que también es una oportunidad para reforzar la confianza y permitir la innovación en el futuro.

Aplicaciones y beneficios reales

La transición a la criptografía poscuántica es más que un ejercicio de cumplimiento normativo; es un imperativo empresarial que afecta directamente a la confianza, la resiliencia y la competitividad a largo plazo. Para los proveedores de telecomunicaciones, las instituciones financieras, las organizaciones de servicios de salud y las agencias gubernamentales, la adopción de algoritmos resistentes a la computación cuántica garantiza que la infraestructura digital crítica siga siendo segura frente a las amenazas tanto actuales como futuras.

Telecomunicaciones

Las redes de telecomunicaciones son la columna vertebral de la digitalización global. Lo permiten todo, desde servicios de emergencia y conectividad de IoT hasta comunicaciones seguras con los clientes. Una filtración cuántica en este sector podría poner en riesgo el aprovisionamiento de SIM, la incorporación de eSIM o los procesos de autenticación que sustentan el 4G y el 5G. Mediante la implementación de criptografía híbrida y con seguridad cuántica hoy, los operadores pueden mantener la confianza de los clientes, proteger la privacidad de los datos y garantizar una continuidad del servicio optimizada en todas las generaciones de tecnología móvil.

Servicios financieros

El sector financiero es uno de los principales objetivos de los ciberatacantes y la integridad de las transacciones depende de la criptografía. La preparación poscuántica protege los pagos digitales, la banca online y las transferencias interbancarias contra el fraude habilitado por la computación cuántica. La adopción temprana también asegura a los reguladores y los clientes que las instituciones se comprometen a proteger los activos y mantener la estabilidad sistémica. La criptografía preparada para el futuro en este sector reduce tanto la exposición normativa como el riesgo para la reputación.

Servicios de salud

Las historias clínicas, los datos genómicos y los dispositivos médicos conectados corren el riesgo de sufrir ataques de tipo "cosechar ahora, descifrar después". El sector de los servicios de salud se enfrenta a un reto adicional: los largos periodos de retención necesarios para los datos médicos confidenciales. Si inician la transición a la PQC hoy, los hospitales y proveedores garantizan que los historiales médicos sigan siendo privados, no solo ahora, sino también décadas en el futuro. Esto es esencial para mantener la confianza de los pacientes y, al mismo tiempo, cumplir con las normativas de protección de datos en constante evolución.

Gobierno e infraestructura crítica

Desde las comunicaciones de defensa hasta los sistemas de distribución de energía, los gobiernos y los operadores de infraestructuras confían en la criptografía para garantizar la continuidad de las operaciones y la seguridad nacional. La criptografía poscuántica protege no solo contra los adversarios a corto plazo, sino también contra la recopilación estratégica de comunicaciones cifradas para su explotación futura. La alineación con marcos como CNSA 2.0 garantiza que los sistemas gubernamentales sigan siendo interoperables, seguros y de confianza en la era cuántica.

Beneficios empresariales más amplios

Aunque la necesidad técnica de PQC es clara, el caso empresarial es igualmente sólido:

- Confianza y reputación de marca: demuestra liderazgo en la protección de los datos de clientes y socios.
- Cumplimiento normativo: se ajusta a los estándares del NIST y a los mandatos gubernamentales, como CNSA 2.0.
- Resiliencia operativa: reduce el riesgo de interrupciones catastróficas causadas por criptografía rota.
- Diferenciación de la competencia: posiciona a las organizaciones como innovadoras proactivas en lugar de seguidoras reactivas.

Los beneficios de actuar ahora van mucho más allá de la resiliencia técnica. Las organizaciones que adopten la PQC de forma temprana no solo reducirán el riesgo, sino que también reforzarán su capacidad para innovar, cumplir y competir en una economía digital que depende de la confianza.

Dé los siguientes pasos

La llegada de la computación cuántica representa tanto una oportunidad generacional como un desafío de seguridad sin precedentes. Aunque los plazos exactos de los ordenadores cuánticos criptográficamente relevantes siguen siendo inciertos, lo que sí es cierto es el esfuerzo necesario para prepararse. La transición a la criptografía poscuántica requerirá años de planificación, inversión y ejecución coordinadas. Esperar a que los ordenadores cuánticos estén operativos no es una opción práctica.

El primer paso para cualquier organización es la concienciación: saber dónde y cómo se utiliza la criptografía en su entorno. A partir de ahí, las empresas deben comenzar el proceso de inventariado, priorización y pruebas piloto de soluciones cuánticas seguras. La criptografía híbrida, que combina algoritmos clásicos y poscuánticos, ofrece una ruta inmediata hacia la resiliencia mientras los estándares siguen evolucionando. Mediante la alineación de los roadmaps internos con los marcos globales, como los estándares de PQC del NIST y los plazos de CNSA 2.0, las organizaciones pueden avanzar con confianza hacia el cumplimiento normativo y la interoperabilidad.

Dell Technologies se compromete a ayudar a los clientes a lidiar con esta transición. A través de nuestro enfoque, ofrecemos una base de integridad de la cadena de suministro, protecciones integradas en hardware y capacidad de adaptación habilitada por software. Nuestras asociaciones con los principales proveedores de seguridad y nuestro papel activo en los organismos de normalización del sector garantizan que las soluciones de Dell no solo se ajusten a los requisitos más recientes, sino que también se prueben para garantizar un rendimiento y una interoperabilidad reales.

Empiece a prepararse hoy mismo. Empiece con el descubrimiento y el análisis de riesgos, colabore con proveedores de confianza y realice pruebas piloto de tecnologías con seguridad cuántica. Cada paso que se da ahora reduce el riesgo de que se produzcan interrupciones en el futuro. Las organizaciones que actúen con anticipación no solo protegerán sus datos y sistemas, sino que también se ganarán la confianza de clientes, reguladores y socios en una era en la que la confianza digital es primordial.

Acerca de nosotros

Dell Technologies se compromete a hacer que la tecnología avanzada sea accesible, fiable e habilitadora para todos. Ayudamos a las personas y las organizaciones a aprovechar la innovación de forma segura, liderando el camino hacia un futuro más seguro, inclusivo y conectado.