DELL Technologies

Criptografía poscuántica

Empezar

INTRODUCCIÓN

La computación cuántica está impulsando un rediseño fundamental de la tecnología, lo que genera oportunidades increíbles y nuevos retos. Aunque el futuro es prometedor, presenta una amenaza importante para los sistemas criptográficos que protegen nuestro mundo digital.

¿Por qué está en auge la computación cuántica?

Los equipos clásicos, ya sean portátiles, teléfonos inteligentes o servidores, procesan la información con 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.

¿Qué es 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.

¿A qué riesgos inmediatos de la computación cuántica se enfrentan las organizaciones?

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 amenaza de "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 ordenadores cuánticos criptográficamente relevantes, los daños ya serán irreversibles.

“Cosechar ahora, descifrar después”, también conocido como "registrar ahora, descifrar después" es el acto por el que los adversarios recopilan y almacenan hoy datos cifrados con la intención de descifrarlos en el futuro, una vez que los ordenadores cuánticos criptográficamente relevantes estén disponibles.

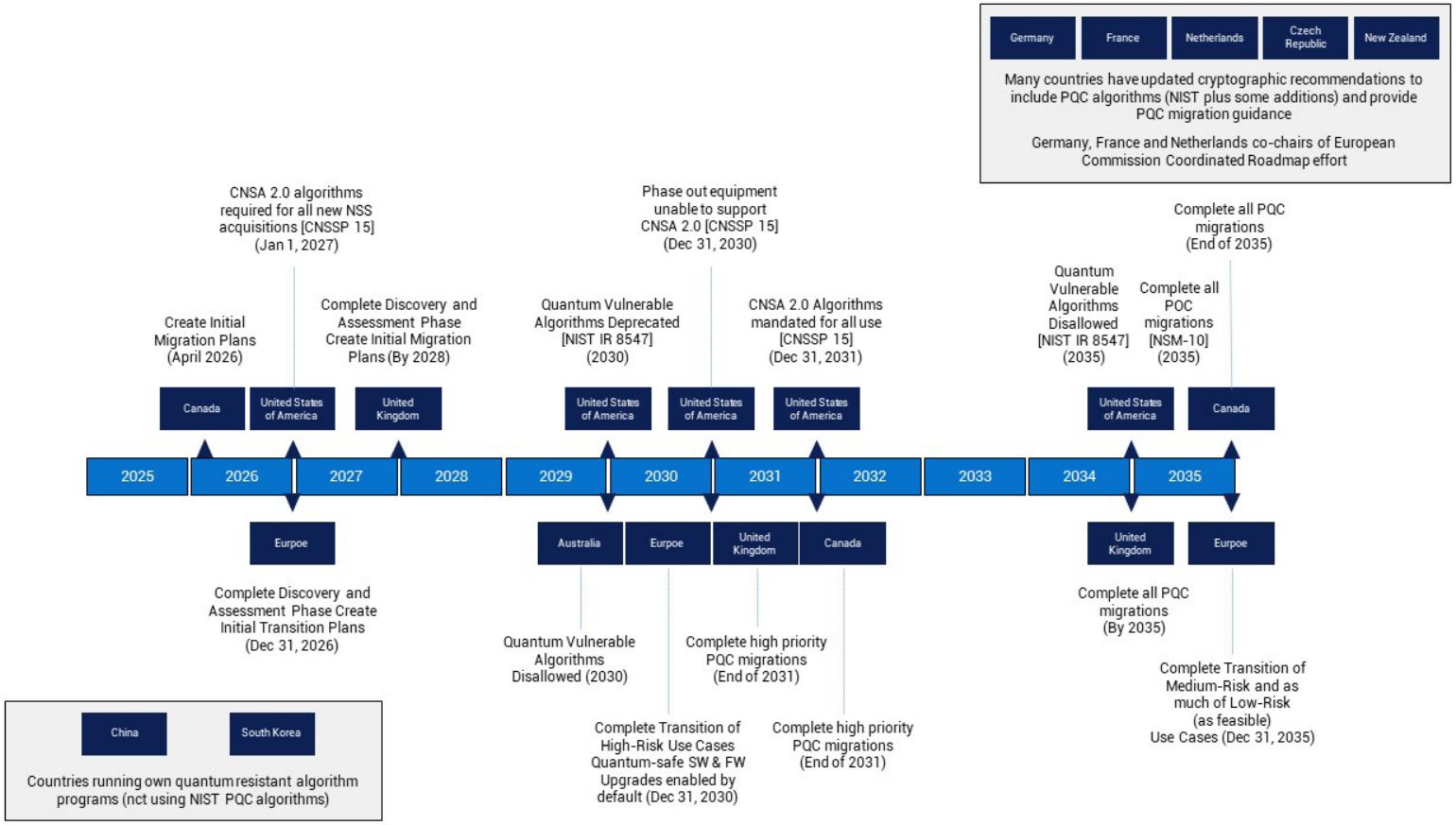
¿Cómo deberían prepararse las organizaciones para la transición a la PQC?

El camino hacia un futuro de seguridad cuántica es una maratón, no un esprint, y con un recorrido en constante evolución. Un enfoque proactivo, por capas y por fases ayudará a su organización a gestionar los riesgos, alinear los recursos y crear un estado de seguridad resiliente a largo plazo. Dell proporciona las tecnologías y la orientación necesarias para ayudarle en cada etapa. Aquí encontrará los pasos clave para guiar a su organización en la creación de un plan de transición hacia la PQC.

Cronograma de transición a la PQC

Reconociendo la urgencia de la amenaza, los gobiernos y los organismos de normalización han convertido la PQC en una prioridad mundial. Conscientes de la importancia de adoptar algoritmos criptográficos 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 el Memorando de Seguridad Nacional 10 (NSM-10), el Conjunto de Algoritmos de Seguridad Nacional Comercial (CNSA 2.0), el Memorando de la Oficina de Administración y Presupuesto 23-02 (OMB M-2302) y el Informe Interagencial del Instituto Nacional de Estándares y Tecnología 8547 (NIST IR 8547).

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



Inventario y auditoría de amenazas criptográficas

La principal prioridad es comprender su panorama criptográfico actual. Este paso básico fundamenta toda su estrategia de migración.

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, para los sistemas más nuevos, aumentar la robustez de seguridad mínima (AES-256 para la criptografía simétrica y SHA-384 o superior para los resúmenes) a fin de 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 amenazas criptográficas

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, datos de clientes, datos archivados, etc. 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

Con un inventario claro, puede comenzar a experimentar de forma práctica con tecnologías preparadas para la PQC a fin de validar su rendimiento e integración.

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 maduran los estándares de PQC, puede comenzar a planificar su implementación en la producción.
Un enfoque híbrido proporciona un puente hacia un entorno cuántico totalmente seguro.

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 empresa con una seguridad cuántica totalmente integrada y validada continuamente.

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 entornos híbridos con ordenadores clásicos y cuánticos, 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

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.

Conclusión

La era cuántica ya no es una posibilidad lejana, sino una realidad inminente que requiere actuar con visión de futuro en la actualidad. Prepararse para este cambio tecnológico es un imperativo estratégico para proteger su activo más valioso: sus datos. Como hemos descrito, un enfoque por fases que pase del inventario y la auditoría a la migración completa es el camino más claro para garantizar un futuro cuántico seguro.

El paso a la PQC 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 transición a la PQC.