Publicado en América Latina el 22/02/2024

# [DigiCert explica cómo controlar los activos para prepararse hacia la computación postcuántica](http://www.notasdeprensa.es)

## Según DigiCert la transición a la criptografía resistente a los cuánticos es una tarea importante. Pero al identificar y administrar los cripto activos, las organizaciones pueden sentar las bases para un futuro digital, seguro y confiable

 La tendencia de la digitalización en todos los sectores se acelera cada vez más. Previsiones, como las de la consultora de datos Statista, apuntan a que en los próximos diez años habrá 50.000 millones de dispositivos conectados, analizando y generando información, lo que dará lugar a un auge aún mayor del Internet de las cosas (IoT). El mayor reto al que se enfrenta la sociedad será aprovechar los datos generados para ponerlos al servicio del desarrollo empresarial, pero estas enormes cantidades de información son casi imposibles de analizar con los ordenadores actuales. Aquí es donde radica la importancia de la computación cuántica para el futuro de la industria 4.0. Sin embargo, la inminente llegada de la computación cuántica está exponiendo lo que los expertos en criptografía ya saben: las criptomonedas están en todas partes. Casi todo lo que implementa prácticas de seguridad modernas se basa en la criptografía y las infraestructuras de clave pública (PKI) para generar confianza digital. El primer paso es comenzar a inventariar los certificados, algoritmos y otros activos criptográficos, priorizándolos según su nivel de importancia. A partir de ahí, se puede determinar qué es necesario actualizar o reemplazar para garantizar que sus sistemas permanezcan seguros cuando la computación cuántica se convierta en una realidad. "El lugar para comenzar a cambiar los algoritmos de cifrado es con criptografía que produce firmas en las que se debe confiar durante mucho tiempo: piense en cosas como raíces de confianza y firmware para dispositivos de larga duración. Y sí, eso significa producir inventarios detallados de software y dispositivos y de dónde provienen sus criptomonedas", explica Dean Coclin,Director senior de desarrollo empresarial de DigiCert. ¿Por qué? Los atacantes están jugando a largo plazo, registrando datos cifrados como parte de una estrategia de vigilancia llamada "cosechar ahora, descifrar después". Cuando la computación cuántica esté disponible, los ciberdelincuentes la descifrarán, y la única manera segura de protegerse contra esta estrategia es priorizar cualquier cifrado del que dependerá su organización a largo plazo. Volverse cripto ágilHacer un inventario de los activos criptográficos darán sus frutos cuando la computación cuántica comience a romper los algoritmos, y aunque no se sabe exactamente cuándo sucederá eso, sí se sabe que es una cuestión de cuándo, no de si sucederá. Una vez que se complete el inventario, la siguiente fase de la transición de PQC será lograr la cripto agilidad, que implica visibilidad de activos, métodos establecidos para implementar tecnologías de cifrado y la capacidad de responder rápidamente cuando surgen problemas de seguridad. La transición a la criptografía resistente a los cuánticos es una tarea importante. Pero al identificar y administrar los cripto activos, las organizaciones puede sentar las bases para un futuro digital, seguro y confiable. Para obtener más información sobre PQC, se puede visitar: https://labs.digicert.com/quantum-safe

**Datos de contacto:**

DigiCert Latam

DigiCert PR Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/digicert-explica-como-controlar-los-activos](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Programación Software Ciberseguridad Innovación Tecnológica Actualidad Empresarial



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)