Publicado en América Latina el 28/10/2024

# [Tres desafíos clave para lograr la criptoagilidad en la era post cuántica](http://www.notasdeprensa.es)

## Un reciente estudio realizado por DigiCert en colaboración con Ponemon Institute reveló que los líderes de TI están cada vez más preocupados por las amenazas que plantea la computación cuántica

  Entre los principales hallazgos del estudio realizado por la empresa se destacan: ●        61% de los líderes de TI en América Latina cree que sus organizaciones no están preparadas para enfrentar las implicaciones de seguridad de la computación cuántica. ●        74% teme que los atacantes utilicen la técnica de "cosechar ahora, descifrar después" para vulnerar datos cifrados en el futuro. ●        La transición hacia la criptografía cuántica segura presenta desafíos significativos en términos de almacenamiento, dispositivos IoT y el reemplazo masivo de claves privadas. En este contexto, DigiCert analiza los tres principales desafíos que enfrentan las organizaciones para lograr la criptoagilidad y cómo pueden superarlos: Desafío #1: Ampliar el tamaño de las claves cuánticas Las claves cuánticas, dependiendo del algoritmo, son hasta diez veces más grandes que las claves RSA tradicionales. Por ejemplo, una clave RSA de 2048 bits tiene 256 bytes de almacenamiento, lo que, aunque manejable, se convierte en un reto cuando se trata de dispositivos con almacenamiento limitado. A medida que ciertas claves basadas en hash pueden escalar hasta gigabytes, la gestión de este espacio adicional se vuelve crítica durante la transición a la seguridad cuántica. Desafío #2: Hacer que los dispositivos IoT sean cuánticamente seguros Los dispositivos IoT están diseñados para durar muchos años, incluso décadas. Sin embargo, con la llegada de las computadoras cuánticas relevantes para la criptografía (CRQC) en los próximos 5 a 10 años, la seguridad de estos dispositivos está en riesgo. Los fabricantes deben garantizar que los dispositivos que se envían hoy sean capaces de resistir las amenazas cuánticas en el futuro. Desafío #3: La escala de los reemplazos de claves privadas Cada dispositivo, aplicación y servicio digital depende de certificados digitales que utilizan claves privadas para garantizar la seguridad. Con el crecimiento exponencial de dispositivos IoT y servicios en la nube, la cantidad de claves privadas también aumenta. Cuando lleguen las CRQC, todas estas claves deberán ser reemplazadas, lo que representa un reto logístico considerable. En este contexto, las empresas necesitan una solución que no solo aborde los desafíos actuales, sino que también proporcione la criptoagilidad necesaria para adaptarse a claves más grandes y complejas en el futuro.

**Datos de contacto:**

PR DigiCert Latam

DigiCert

312000000

Nota de prensa publicada en: [https://www.mexicopress.com.mx/tres-desafios-clave-para-lograr-la](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Finanzas Programación Software Ciberseguridad Recursos humanos Consumo Criptomonedas-Blockchain Otras Industrias Innovación Tecnológica Digital



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