Evaluación de la Preparación para la Transición Post-Cuántica

La amenaza cuántica

La computación cuántica está transformando rápidamente el panorama de la ciberseguridad. Algoritmos como RSA y ECC, que actualmente protegen las comunicaciones digitales, los sistemas financieros y la verificación de identidad, dejarán de ser seguros frente a ataques cuánticos. Esto introduce una vulnerabilidad crítica: los datos cifrados interceptados hoy podrían ser descifrados en el futuro, un escenario conocido como "harvest now, decrypt-later".

No se trata de una preocupación lejana o especulativa. La Comisión Europea, NIST y CCN-PYTEC han publicado calendarios de migración y recomendaciones estratégicas muy concretas. No actuar hoy incrementa la deuda criptográfica y la exposición operativa, poniendo en riesgo la confidencialidad y autenticación a largo plazo, pilares fundamentales de la confianza digital.

La transición post-cuántica

La Criptografía Post-Cuántica (PQC) ofrece un camino estratégico hacia la protección frente a ataques cuánticos, con algoritmos diseñados específicamente para resistirlos. Sin embargo, la transición hacia una criptografía resistente frente a la computación cuántica es un desafío complejo que requiere años de planificación coordinada, descubrimiento interno y priorización de riesgos.

Esta transición no es solo una necesidad técnica, es también una capacidad estratégica. Las organizaciones deben identificar dónde se utiliza la criptografía, evaluar la criticidad y la vida útil de los datos protegidos, y comprender las dependencias entre sistemas. Prepararse con antelación permite a las compañías migrar a su propio ritmo, evitar despliegues apresurados e incorporar la cripto-agilidad en su arquitectura.

La fase de preparación es esencial: permite a las organizaciones alinearse con estándares internacionales, anticipar requisitos regulatorios y fortalecer la resiliencia de su infraestructura digital.

Servicios para la Transición Post-Cuántica en Applus+ Laboratories

Applus+ Laboratories ofrece un servicio estructurado para apoyar a las organizaciones en su transición hacia la seguridad cuántica. Nuestra metodología está diseñada para ayudar a los equipos a obtener claridad, definir prioridades y establecer una estrategia de migración segura.

Inventariado Criptográfico

Comenzamos identificando y clasificando los usos de la criptografía en tu organización. Esto incluye identificar dónde se utiliza la criptografía, qué algoritmos están desplegados y qué sistemas protegen la información sensible. El resultado es una Lista de Materiales Criptográficos (Cryptographic Bill of Materials - CBOM) que destaca los activos críticos y los datos que requieren protección a largo plazo, sirviendo como base para una planificación estratégica sólida.

Evaluación de Riesgos Cuánticos

A continuación, analizamos el impacto potencial de la computación cuántica en tu entorno. Priorizamos los sistemas con mayor exposición: aquellos que protegen información sensible de larga vida útil, utilizan criptografía heredada o dependen de terceros. El resultado es un perfil de riesgo claro y priorizado que guía la hoja de ruta de transición.

Definición de la Hoja de Ruta Post-Cuántica

Finalmente, te ayudamos a definir un plan de migración por fases, alineado con los estándares internacionales. Esta hoja de ruta traduce los riesgos en acciones concretas, establece plazos realistas y minimiza las interrupciones operativas. Permite a los equipos internos ejecutar con confianza y garantiza la seguridad y el cumplimiento a largo plazo.

Por qué elegir Applus+ Laboratories para tu transición a la ciberseguridad post-cuántica

En Applus+ Laboratories contamos con amplia experiencia en evaluación criptográfica y garantía de seguridad. Durante años, hemos ayudado a organizaciones de distintos sectores a evaluar y validar sus mecanismos criptográficos conforme a múltiples marcos normativos y esquemas de certificación.

Nuestro equipo incluye expertos en criptografía post-cuántica y participa activamente en grupos nacionales e internacionales de ciberseguridad.

Acompañamos a las organizaciones que se enfrentan a escenarios complejos, ayudándolas a prepararse para la era cuántica. Nuestros servicios complementan las estrategias internas, se alinean con los estándares en evolución y refuerzan la confianza digital.

Al elegir Applus+ Laboratories, obtienes un socio comprometido con ayudarte a afrontar la transición post-cuántica con confianza, claridad y cumplimiento.