LITORALPRESS

Fecha: 28-12-2024
Medio: La Tribuna
Supl. : La Tribuna
Tipo: Noticia general
Título: El futuro de los datos: Seguridad en un mundo cuántico

Pág. : 2
Cm2: 235,3

Tiraje: 3.600
Lectoría: 14.800
Favorabilidad: No Definida

El futuro de los datos: Seguridad en un mundo cuántico

Paulina Assmann
CEO de SeQure Quantum y experta de la Comisión asesora sobre Tecnologías Cuánticas en Chile.

El reciente lanzamiento del chip cuántico de Google, "Willow", ha puesto nuevamente en la palestra los avances y desafíos que trae consigo la computación cuántica. El panorama tecnológico se proyecta revolucionario para el 2025, con innovaciones transformadoras en diversas áreas que destacan a la cuántica como una de las protagonistas. Sin duda se trata de un escenario emocionante, pero no por eso exento de complejidades. Mientras el mundo celebra este progreso como un adelanto hacia un futuro más conectado y eficiente, también surgen preguntas inevitables: ¿estamos preparados para los riesgos que esto implica?

Uno de los principales peligros asociados con el avance de la Inteligencia Artificial y la computación cuántica es su capacidad para amenazar las bases de la ciberseguridad tal como las conocemos. Los algoritmos de cifrado actuales, que protegen transacciones bancarias, datos médicos y comunicaciones críticas, podrían quedar obsoletos frente a la potencia de un computador cuántico plenamente desarrollado. Esta realidad ha dado lugar al desarrollo de algoritmos de criptografía post-cuántica (PQC, por sus siglas en inglés), diseñados para resistir ataques de esta índole, lo que marca una nueva etapa en la defensa de la información sensible.

En este contexto, vale la pena reflexionar sobre el rol que juegan hoy los números pseudoaleatorios en la ciberseguridad. Los sistemas de cifrado actuales dependen de estos para generar claves que, idealmente, sean imposibles de predecir. Sin embargo, la combinación de IA y computación cuántica podría comprometer esa imprevisibilidad; En el futuro, estos avances tendrán el potencial de acelerar la capacidad de descifrar dichas claves, poniendo en jaque la seguridad de datos a nivel global.

Por ello, la transición hacia tecnologías más robustas no es opcional, sino urgente. En el caso de la criptografía post-cuántica, su adopción plantea tanto una solución como un desafío. Si bien promete blindar nuestras estructuras digitales frente a amenazas futuras, su implementación masiva requiere una coordinación significativa entre industrias, gobiernos y comunidades científicas. Esto teniendo en cuenta, además, que el periodo de transición podría representar una ventana de vulnerabilidad considerable.

Desde Sequre Quantum, hemos trabajado en el desarrollo de tecnologías que no solo responden a esta necesidad, sino que lo hacen con un enfoque innovador. Nuestro generador cuántico de números aleatorios (SeQRNG) ofrece una base más segura para la creación de claves criptográficas, garantizando una aleatoriedad que supera ampliamente la de los métodos tradicionales y eleva los estándares de seguridad para enfrentar amenazas emergentes.

A pesar de esto, no debemos perder de vista que la tecnología por sí sola no es suficiente. Es crucial complementar estas innovaciones con una mayor conciencia sobre los riesgos inherentes y una cultura de ciberseguridad que priorice la anticipación sobre la reacción: Safe now and decrypt later.

Como en toda revolución tecnológica, la computación cuántica ofrece tanto oportunidades como desafíos. La clave estará en nuestra capacidad para abordar ambos de manera equilibrada. En un momento donde tecnologías como "Willow" capturan la atención global, recordemos que cada avance trae consigo una responsabilidad. La seguridad en la era cuántica no será el resultado de una solución única, sino de un esfuerzo colectivo que combine innovación, colaboración y un compromiso constante con la protección de datos críticos. Solo así podremos aprovechar al máximo los beneficios de esta nueva frontera tecnológica, minimizando sus riesgos.