La amenaza cuántica. El día “Q” y sus implicaciones para la seguridad global

DOI: 10.29236/sistemas.n173a6

Resumen
El “Día Q” marca un punto de inflexión en la ciberseguridad global: el día en que las computadoras cuánticas tengan la capacidad de romper los algoritmos criptográficos clásicos, que protegen gran parte de la información sensible a nivel mundial. Aunque la llegada precisa de este día es incierta, las fuentes coinciden en que la amenaza es real y requiere una acción inmediata por parte de Estados y organizaciones. Esta breve reflexión hace una revisión los desafíos claves de esta amenaza cuántica revisando algunos de los algoritmos vigentes para la seguridad de las comunicaciones por internet, los retos de la migración a algoritmos poscuánticos y el plan de migración que se debe concretar para limitar las consecuencias por la materialización de esta amenaza. En este sentido, la planeación estratégica, la colaboración y una visión integral se convierten en el marco de trabajo básico para disminuir la amenaza, reducir la vulnerabilidad y mitigar los impactos para hacer más resiliente la infraestructura de seguridad y control global y empresarial.

Palabras clave
Computación cuántica, cúbits, seguridad global, Día Q, amenaza cuántica

Introducción

La computación cuántica aparece en el escenario como un nuevo paradigma en ciencias de la computación que aprovecha los principios de la mecánica cuántica para resolver problemas complejos que están más allá de las capacidades de los computadores tradicionales. En este contexto, a diferencia de estos computadores, que almacenan información en bits que representan 1 o 0, las computadoras cuánticas utilizan qubits (cúbits). Los qubits pueden representar 0 o 1 o una combinación de ambos estados al mismo tiempo, un fenómeno conocido como superposición, lo que habilita a estas máquinas a trabajar de forma masiva en paralelo, explorando múltiples posibilidades a la vez (Shafique et al., 2024).

Este novedoso avance de la ciencia abre fuentes inexploradas de oportunidades que pueden generar avances importantes en diferentes disciplinas como: (Kietzmann et al., 2021)

- Ciencias de la salud y la vida: desarrollo de nuevos medicamentos, terapias de medicina de precisión, estudios de asociación de genoma completo.

- Energía: prevención y resolución de interrupciones en el servicio de energía, optimización de la red eléctrica.

- Logística: optimización de rutas, reducción de emisiones de gases de efecto invernadero.

- Ciencias de los materiales: diseño de nuevos materiales.

- Finanzas: análisis de riesgos, fijación de precios de derivados, detección de fraudes, puntuación de crédito/activos.

- Ciberseguridad: desarrollo de algoritmos criptográficos resistentes a la computación cuántica.

Sin perjuicio de lo anterior, la computación cuántica funda amenazas importantes a la seguridad digital comoquiera que las comunicaciones y transacciones globales ahora basadas en algoritmos de criptografía clásica, podrán ser superados una vez se alcance el momento donde esta computación se encuentre completamente confiable y funcional. Con los avances que se presentan en la actualidad para concretar una computación cuántica funcional, las naciones y organizaciones requieren avanzar rápidamente en planes de migración a esquemas de protección poscuánticas (PQC – *Post Quantum Computing*) que anticipen los posibles riesgos anunciados (Bhat et al., 2022).

En este sentido, la experiencia previa del “Y2K”, puede ser útil para

avanzar con celeridad en este contexto, para lo cual es importante capitalizar lecciones aprendidas como: (Vermeer & Peet, 2020)

- *Riesgo del ataque "cosechar ahora y descifrar después":* si se almacena información sensible y cifrada en la actualidad y el día "Q" llegase a tiempo, se produciría un incalculable perjuicio de consecuencias difíciles de calcular (Amos, 2024).

- *Actuación de forma temprana*: Cuanto más tiempo espere una organización para comenzar la migración a PQC, mayor será el riesgo y la complejidad de la transición.

- *Colaboración entre sectores*: La coordinación entre gobiernos, industria y la comunidad de investigación es crucial para desarrollar, estandarizar e implementar soluciones PQC efectivas.

- *Planificación y la evaluación de riesgos*: Las organizaciones deben evaluar su exposición a la amenaza cuántica, identificar sistemas y datos críticos, y desarrollar planes de migración integrales.

Por tanto, este breve artículo presenta una revisión de la amenaza cuántica situada en el día "Q", esto es, el momento en el futuro cuando los computadores cuánticos sean lo suficientemente robustos como para romper los algoritmos criptográficos asimétricos y debilitar los simétricos clásicos que actualmente protegen la información sensible en línea (Chen et al., 2016) para lo cual es necesario entender los desafíos propios en la computación cuántica, los algoritmos cuánticos utilizados en la actualidad, el reto de la migración hacia algoritmos poscuánticos y el plan de migración que tanto naciones como organizaciones deben emprender para anticipar este momento que tarde o temprano cambiará la dinámica de la seguridad global.

Desafíos actuales de la computación cuántica

La computación cuántica enfrenta diversos retos que la comunidad científica internacional viene afrontando con el fin de aprovechar toda su potencialidad y concretar la promesa de cambio y transformación de la computación actual. Algunos de ellos se detallan a continuación: (Pupillo et al., 2023)

- *Fragilidad de los cúbits* - Los qubits son extremadamente sensibles a las perturbaciones ambientales, como los campos electromagnéticos, y requieren condiciones extremas para mantener su estabilidad, como temperaturas cercanas al cero absoluto (- 273.15 grados Celsius)

- *Escalabilidad y corrección de errores* - A medida que aumenta el número de cúbits, también lo

hace la complejidad de las interacciones entre ellos y la susceptibilidad a los errores.

- *Desarrollo de algoritmos cuánticos* - Si bien se han logrado avances significativos en el desarrollo de algoritmos para problemas específicos, como la factorización y la búsqueda, la exploración de nuevas aplicaciones y la optimización de los algoritmos existentes son áreas de investigación activa.

- *Retos para la ciberseguridad* – En este contexto los desafíos se centran en: romper los criptosistemas actuales, la transición a la criptografía poscuántica, y la evaluación de riesgos y la planeación de la migración lo que implica un trabajo coordinado en las organizaciones.

- *Acceso equitativo* – Asegurar un acceso equitativo a la computación cuántica es importante para fomentar la innovación y evitar la concentración del poder en manos de unos pocos.

Estos desafíos requieren importantes recursos financieros y experiencia especializada que implica no sólo formación de alto nivel sino instalaciones dedicadas con equipo específico que por lo general requiere apoyo de los proveedores y las alianzas necesarias con los gobiernos y universidades para lograr el desarrollo de las aplicaciones o proyectos de investigación. Así mismo, Iniciativas como el *Open Quantum Institute* promueven el acceso abierto a los recursos cuánticos con el fin de motivar una colaboración global (Pupillo et al., 2023)

Lo anterior implica un cambio fundamental en la forma que se generan los algoritmos de programación y particularmente para los temas criptográficos la comprensión de una dinámica de protección basada en el tratamiento de los cúbits que se ve reflejada particularmente en los algoritmos de Shor y Grover.

Los algoritmos cuánticos utilizados en la actualidad

Si bien existen múltiples algoritmos utilizados para concretar diferentes proyectos de investigación y avances relevantes en diferentes temáticas, a continuación se presenta un resumen de aquellos que resultan de interés en la actualidad dada sus referencias en estudios científicos recientes (Shafique et al., 2024).

Particularmente para los efectos de este documento se hará énfasis en los algoritmos de Shor y de Grover dado que son los que en la actualidad se concentra la amenaza cuántica que busca romper los criptosistemas clásicos generalmente basado en RSA (*Rivest Shamir Adleman*) y curvas elípticas (ECC-*Elliptic Curve Cryptography*).

El algoritmo de Shor, fue desarrollado por el Dr. Peter Shor, profesor

Tabla 1.
Algunos algoritmos cuánticos. Características y aplicaciones

Algoritmo Cuántico	Características Claves	Aplicaciones
Algoritmo de Shor	· Factoriza números grandes y resuelve los problemas de búsqueda de orden multiplicativo y logaritmo discreto en tiempo polinomial. · Representa una amenaza significativa para los criptosistemas actuales basados en RSA (*Rivest Shamir Adleman*) y ECC (*Elliptic Curve Cryptography*).	· Criptoanálisis (romper el cifrado RSA y ECC). · Resolución de problemas matemáticos basados en factorización y otros vinculados.
Algoritmo de Grover	· Busca en una base de datos no ordenada en tiempo O(√N). · Ofrece una aceleración cuadrática sobre los algoritmos clásicos de búsqueda. · Para la criptografía simétrica y funciones “hash” (digesto), se impone el aumento del tamaño de las claves y parámetros vinculados.	· Búsqueda de datos en grandes bases de datos. · Aceleración de algoritmos de aprendizaje automático. · Resolución de problemas de optimización.
Algoritmo de Deutsch-Jozsa	· Determina si una función booleana es constante o balanceada con una sola consulta. · Supera a los algoritmos clásicos que requieren múltiples consultas para resolver el mismo problema.	· Demostración de la ventaja cuántica en la resolución de problemas específicos. · Aplicaciones en teoría de la computación.
QAOA (Quantum Approximate Optimization Algorithm)	· Un algoritmo híbrido cuántico-clásico para resolver problemas de optimización combinatoria. * Potencial para encontrar soluciones aproximadas a problemas difíciles.	· Optimización de carteras financieras. · Diseño de materiales. · Logística y planificación.
QSVM (Quantum Support Vector Machines)	· Una versión cuántica del algoritmo de aprendizaje automático de máquinas de vectores de soporte (SVM). · Potencial para mejorar la precisión y la eficiencia del aprendizaje automático.	· Clasificación de datos. · Reconocimiento de patrones. · Análisis de imágenes.

Nota: Basado en: Shafique et al., 2024

de matemáticas del MIT en 1994. Es un algoritmo cuántico relevante por su capacidad para factorizar números grandes y otros problemas numéricos vinculados en tiempo polinomial (tiempo de ejecución de un algoritmo (mediante el cual se obtiene una solución al problema) es menor o igual que un cierto valor calculado a partir del número de variables implicadas (generalmente variables de entrada) usando una fórmula polinómica o polinomio. Esta capacidad tiene implicaciones significativas para la ciberseguridad, ya que puede romper los esquemas de cifrado de clave pública ampliamente utilizados, como RSA, que se basan en la dificultad de factorizar números grandes (Clark et al., 2021).

El algoritmo de Shor se basa en conceptos clave de la mecánica cuántica: (Shafique et al., 2024)

- Superposición: Los cúbits pueden existir en una superposición de estados, es decir, pueden estar en el estado 0, en el estado 1 o en una combinación de ambos al mismo tiempo.

- Entrelazamiento: Dos o más cúbits pueden estar entrelazados, lo que significa que sus estados están supercorrelacionados (con entropía negativa), incluso si están infinitamente separados en tiempo y espacio.

- Transformada rápida de Fourier (FFT): el mérito principal de Shor fue el descubrimiento de un circuito cuántico que resuelve en tiempo polinomial el problema de la búsqueda de orden multiplicativo de enteros en grupos numéricos, el cual con métodos clásicos es de tiempo exponencial, o sea prácticamente incomputable (Nielsen & Chuang, 2010).

En la medida que se construyan computadores cuánticos más confiables y potentes el algoritmo de Shor tendrá mejores condiciones para concretar su amenaza sobre los criptosistemas mencionados previamente.

Mosca (2018) plantea la pregunta retadora: "¿Cuántos cúbit físicos necesitaremos para romper el RSA-2048? (...) Las estimaciones actuales oscilan entre decenas de millones y mil millones de cúbit físicos". Investigaciones posteriores indican que "en los cuatro años transcurridos desde 2015, el extremo superior de la estimación de cuántos cúbits serán necesarios para factorizar los enteros RSA de 2048 bits ha caído casi dos órdenes de magnitud; de mil millones a veinte millones" (Gidney & Ekerå, 2021).

A la fecha existe un reciente avance muy prometedor, el desarrollo de cúbits libre de errores, lo que haría caer esta última estimación otros dos o tres órdenes de magnitud que es lo que actualmente persiguen grandes actores como Google

(Shankland, 2020). De concretarse, el día "Q" estaría muy cercano.

De otra parte, el algoritmo de Grover, propuesto por Lov Grover en 1996, es un algoritmo cuántico que destaca por su capacidad para buscar un elemento específico en una base de datos no ordenada de tamaño N con una complejidad temporal de $O(\sqrt{N})$. Esto contrasta con los algoritmos clásicos de búsqueda, que requieren un tiempo de O(N) en el peor de los casos (Grover,1996).

El algoritmo de Grover se basa en los siguientes elementos: (Grover, 1996)

- Superposición: Al igual que el algoritmo de Shor, el algoritmo de Grover aprovecha la superposición cuántica. Inicialmente, se crea una superposición que representa todos los posibles elementos de la base de datos.

- Amplificación de Amplitud: El algoritmo aplica una serie de operaciones para amplificar la amplitud de probabilidad del estado que corresponde al elemento buscado.

- Operador de Oráculo: Un componente crucial del algoritmo es el operador de oráculo, que identifica el elemento objetivo. El oráculo invierte la fase del estado que representa el elemento buscado, sin revelar su ubicación.

- Operador de Difusión: El operador de difusión aumenta la amplitud del estado objetivo al invertir los estados alrededor del promedio de las amplitudes.

Si bien el algoritmo de Grover no proporciona una solución en tiempo polinomial para los problemas NP-completos (una clase de problemas computacionales para los cuales no se ha encontrado una solución eficiente, pero si se encontrara una solución, podría verificarse de manera eficiente), ya que la aceleración es cuadrática y no exponencial, sí ofrece una ventaja significativa sobre los algoritmos clásicos para ciertos problemas de búsqueda y optimización, por ejemplo un ataque de fuerza bruta a los algoritmos simétricos (AES) (Shafique et al., 2024).

El día "Q". La migración hacia algoritmos poscuánticos

La urgencia de la migración hacia los algoritmos poscuánticos se ha concretado en un marco de trabajo planteado por Mosca (2018) denominado la desigualdad de Mosca que se basa en tres variables: (Mosca, 2018)

- Tiempo de migración (M): El tiempo que tarda una organización en implementar completamente un criptosistema poscuántico. Este proceso incluye la selección de algoritmos apropiados, la actualización de sistemas y software, la capacitación del personal y las pruebas exhaustivas.

- Vida útil de la seguridad (S): El tiempo que la información en cuestión debe permanecer confidencial. Esto varía según el tipo de información: datos financieros o de salud pueden requerir protección durante décadas, mientras que otros datos pueden tener una vida útil más corta.

- Tiempo de colapso (C): El tiempo estimado hasta que se construya una computadora cuántica criptográficamente relevante (CRQC) capaz de romper los algoritmos criptográficos actuales.

La desigualdad de Mosca establece que si M + S > C, es decir, si el tiempo de migración más la vida útil de la seguridad es mayor que el tiempo de colapso, entonces una organización corre el riesgo de que sus datos sean descifrados en el futuro por una CRQC. En otras palabras, si no se migra a la criptografía poscuántica a tiempo, la información sensible podría volverse vulnerable a ataques una vez que las CRQC estén disponibles.

Lo anterior sugiere que el tiempo de migración previsto para toda una nación será significativamente mayor que el tiempo establecido para una organización. Esto implica que se deben articular esfuerzos entre los distintos sectores de la sociedad con el fin de aumentar la conciencia situacional sobre esta amenaza de mediano plazo para establecer un plan de migración coordinado que permita mejorar la postura de ciberseguridad empresarial de las organizaciones. Es claro que habrá sectores más expuestos que otros y por tanto, aquellos que soportan servicios críticos esenciales estarán en los primeros lugares (Mulholland et al., 2017).

Si bien la amenaza cuántica no sólo está centrada en el descifrado de los datos, igualmente podrá utilizarse para violar mecanismos de autenticación, superar firmas digitales y protocolos de confidencialidad disponibles a la fecha. La desigualdad de Mosca se debe usar como una guía en la toma de decisiones sobre los algoritmos criptográficos actuales, ya que existen muchos inciertos en las estimaciones alrededor de las tres variables que la componen.

Es importante anotar que el día “Q” (que según cálculos actuales llegará a finales de esta década o antes) tendrá graves implicaciones para diferentes sectores de la sociedad. Entre ellos están: (Vermeer & Peet, 2020)

- Seguridad nacional: la información clasificada y las comunicaciones militares podrían verse comprometidas.

- Servicios financieros: las transacciones bancarias y los datos financieros personales podrían ser robados o manipulados.

- Infraestructura crítica: los sistemas de control de la red eléctri-

ca, las telecomunicaciones y otros servicios esenciales podrían ser vulnerables a ataques.

- Privacidad personal: las historias médicas, los registros financieros y otros datos personales confidenciales podrían quedar expuestos.

Plan de migración a algoritmos poscuánticos. Retos para las organizaciones

La migración a algoritmos poscuánticos debe ser un proceso continuo que requiere adaptación y flexibilidad a medida que la tecnología cuántica avanza. En este sentido, las organizaciones y los países deben adelantar una planificación cuidadosa y una ejecución estratégica que permita de manera ordena establecer un plan de acción que termine fortaleciendo la postura de ciberseguridad de la empresa (Mckinsey, 2021).

Siguiendo las reflexiones de Hasan et al. (2024) y Pupillo et al. (2023) se detalla a continuación una propuesta de un plan de migración práctico para considerar frente a la amenaza cuántica:

1. Conciencia y Educación:

a. Comprender la amenaza cuántica: Es fundamental que las organizaciones comprendan la amenaza que representan los computadores cuánticos para los algoritmos criptográficos actuales. Este conocimiento debe extenderse a todos los niveles de la organización, desde la alta dirección hasta el personal de TI.

b. Conocer los algoritmos PQC: Familiarizarse con los diferentes tipos de algoritmos PQC, sus fortalezas, debilidades y casos de uso.

2. Inventario Criptográfico:

a. Identificar activos criptográficos: Crear un inventario completo de todos los activos criptográficos utilizados en la organización, incluyendo algoritmos, claves, certificados, protocolos y sistemas de gestión de claves. Este inventario debe incluir software, hardware, comunicaciones y servicios de terceros.

b. Analizar dependencias: Evaluar las dependencias entre los activos criptográficos y los datos que protegen. Este análisis debe considerar el flujo de datos dentro de la organización y las interacciones con sistemas externos.

3. Evaluación de Riesgos:

a. Determinar la sensibilidad de los datos: Clasificar los datos según su sensibilidad y el tiempo que deben permanecer protegidos.

b. Evaluar el impacto de la computación cuántica: Analizar el impacto potencial de las computadoras cuánticas en los activos criptográficos y los datos, utili-

zando herramientas como la desigualdad de Mosca.

c. Identificar prioridades de migración: Priorizar los sistemas y datos que requieren migración inmediata, basándose en la evaluación de riesgos. Los sistemas con una vida útil prolongada, como la infraestructura y los dispositivos IoT, deben ser priorizados.

4. Selección de Algoritmos PQC:

a. Investigar algoritmos PQC: Investigar y evaluar los algoritmos PQC candidatos que cumplan con los requisitos de seguridad y rendimiento de la organización.

b. Considerar la estandarización: Priorizar los algoritmos PQC que están siendo considerados para la estandarización por organismos como NIST.

c. Adoptar un enfoque híbrido: Considerar el uso de esquemas híbridos que combinen algoritmos clásicos con algoritmos PQC para asegurar una transición fluida y minimizar los riesgos. Estas soluciones parecen ser muy prometedoras para la protección casi inmediata de redes corporativas.

5. Implementación y Prueba:

a. Planificar la implementación: Desarrollar un plan de implementación detallado que incluya pruebas, capacitación y gestión de cambios.

b. Implementar algoritmos PQC: Implementar los algoritmos PQC seleccionados en los sistemas prioritarios, asegurando la interoperabilidad con los sistemas existentes.

c. Probar y validar: Probar y validar exhaustivamente la seguridad y el rendimiento de los sistemas migrados.

6. Monitoreo y Actualización:

a. Monitorear el panorama de amenazas: Monitorear continuamente el panorama de amenazas cuánticas y las actualizaciones de los estándares PQC.

b. Mantener la agilidad criptográfica: Diseñar sistemas con agilidad criptográfica para facilitar futuras actualizaciones y transiciones a nuevos algoritmos.

Conclusiones

La computación cuántica, aunque aún se encuentra en desarrollo, presenta una amenaza potencial significativa para la seguridad global a largo plazo. Los algoritmos cuánticos, como el algoritmo de Shor, tienen la capacidad de romper los criptosistemas ampliamente utilizados hoy en día, como RSA y ECC, que protegen la información confidencial en varios sectores, incluyendo finanzas, sector sanitario y gobierno y debilitar los criptosis-

temas simétricos y las funciones de digesto. (Brooks, 2023; Keary, 2023).

Por tanto, la amenaza cuántica establece una serie de retos para los países y las organizaciones en el mediano plazo, que no sólo van a afectar el cifrado de los archivos, sino crear efectos de orden nacional donde información sensible podrá estar expuesta en el futuro.

En esta línea, esta amenaza se puede dividir en dos momentos: (Tan et al., 2023)

- Recolección de datos actual ("cosecha ahora, descifra después"), como ya fuese mencionado: Los adversarios pueden estar recolectando datos cifrados hoy con la expectativa de que las computadoras cuánticas futuras puedan descifrarlos. Esta táctica subraya la urgencia de la acción, ya que los datos sensibles recopilados hoy podrían estar en riesgo en el futuro. Esta estrategia se puede estar usando hoy por diferentes países desarrollados para contar con información estratégica y determinante en sus esquemas de defensa o propiedad intelectual.

- Descifrado de datos: Una vez que las computadoras cuánticas alcancen la madurez, podrían usarse para descifrar datos cifrados previamente con algoritmos vulnerables a la computación cuántica.

De otra parte, las organizaciones deberán hacer su ejercicio para anticipar esta amenaza para lo cual el plan de migración a algoritmos poscuánticos será parte de la estrategia a seguir, sin perjuicio de la evaluación e impactos jurídicos que se puedan dar frente a eventuales ataque exitosos (acceso a información con deber de protección legal) sobre información cifrada con algoritmos clásicos que posiblemente no terminaron de migrarse o quedaron por fuera de los inventarios realizados. En este contexto pensar en ampliar las pólizas cibernéticas actuales en este sentido, podría ser una oportunidad para ajustar estos ejercicios de riesgos emergentes para las empresas.

Así las cosas, la materialización de la amenaza cuántica en las compañías deberá ser parte de los análisis de riesgos empresariales teniendo en cuenta situaciones como: (Vermeer & Peet, 2020)

- Pérdida de datos confidenciales: Esto podría incluir información financiera, propiedad intelectual, datos de clientes e información estratégica.

- Daño a la reputación: Una violación de datos exitosa debido a la computación cuántica podría dañar la reputación de su organización y erosionar la confianza de los clientes.

- Incumplimiento normativo: La incapacidad para proteger los da-

tos contra las amenazas cuánticas podría resultar en multas y sanciones por incumplimiento de las regulaciones de protección de datos.

- Interrupción operativa: Los sistemas críticos que dependen de la criptografía podrían verse afectados, lo que provocaría interrupciones operativas.

La amenaza cuántica es real y el día "Q" se acerca. En consecuencia, las organizaciones deben tomar las medidas proactivas necesarias y suficientes para prepararse frente a los nuevos escenarios de la computación cuántica y proteger sus datos de las amenazas futuras. La amenaza cuántica es semejante al dilema del volcán, es imperativo estar preparado para cuando se haga realidad, para lo cual habrá que estar atento a los avances y noticias del entorno (favorables frente a la resistencia de los algoritmos poscuánticos, así como de los adversarios en el aprovechamiento y uso adverso de estos algoritmos), mientras se avanza en la migración interna para disminuir las vulnerabilidades e impactos que se puedan tener en el futuro.

La inacción frente a esta realidad podrá tener consecuencias desfavorables significativas y por tanto, acompañarse de expertos en ciberseguridad y computación cuántica para obtener orientación y asistencia se convierte en un elemento estratégico y funcional para articular los esfuerzos de aseguramiento y control frente a un entorno cada vez más hostil y competitivo.

Agradecimientos

El autor agradece al doctor Juan Pedro Hecht, Profesor titular y *Research Fellow* en criptografía de la Universidad de Buenos Aires, Argentina, por sus valiosos y acertados comentarios, los cuales permitieron afinar las reflexiones de este artículo.

Referencias

Amos, Z. (2024). *"Harvest now, decrypt later": Why hackers are waiting for quantum computing*. VentureBeat. https://venturebeat.com/security/harvest-now-decrypt-later-why-hackers-are-waiting-for-quantum-computing/

Bhat, H. A., Khanday, F. A., Kaushik, B. K., Bashir, F., & Shah, K. A. (2022). Quantum computing: Fundamentals, implementations and applications. *IEEE open journal of nanotechnology*, *3*, 61–77. https://doi.org/10.1109/ojnano.2022.3178545

Brooks, C. (2023). *Quantum Tech Needed To Secure Critical Data From Quantum Decryption*. Forbes. https://www.forbes.com/sites/chuckbrooks/2023/01/19/quantum-tech-needed-to-secure-critical-data-from-quantum-decryption/

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.IR.8105

Clark, R., Bartlett, S., Bremner, M., Lam, P. K., & Ralph, T. (2021). *The impact of quantum technologies on secure communications*. Australian Strategic Policy Institute - ASPI. https://www.aspi.org.au/report/impact-quantum-technologies-secure-communications

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*(433), 433. https://doi.org/10.22331/q-2021-04-15-433

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* - STOC '96. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/237814.237866

Hasan, K. F., Simpson, L., Baee, M. A. R., Islam, C., Rahman, Z., Armstrong, W., Gauravaram, P., & McKague, M. (2024). A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE access: practical innovations, open solutions*, *12*, 23427–23450. https://doi.org/10.1109/access.2024.3360412

Keary, T. (2023). *IBM: Quantum computing poses an 'existential threat' to data encryption*. VentureBeat. https://venturebeat.com/security/ibm-quantum-computing/

Kietzmann, J., Demetis, D. S., Eriksson, T., & Dabirian, A. (2021). Hello quantum! How quantum computing will change the world. *IT Professional*, *23*(4), 106-111. https://doi.org/10.1109/MITP.2021.3086917

Mckinsey. (2021). Quantum computing: An emerging ecosystem and industry use cases. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20use%20cases%20are%20getting%20real%20what%20you%20need%20to%20know/quantum-computing-an-emerging-ecosystem.pdf

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE security & privacy*, *16*(5), 38–41. https://doi.org/10.1109/msp.2018.3761723

Mulholland, J., Mosca, M., & Braun, J. (2017). The day the cryptography dies. *IEEE security & privacy*, *15*(4), 14–21. https://doi.org/10.1109/msp.2017.3151325

Nielsen, M. A. & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. 10th Anniversary Edition. Cambridge: Cambridge University Press.

Pupillo, L., Ferreira, A., Lipiainien, V. & Polito, C. (2023), *Quantum Technologies and Cybersecurity: Technology, governance and policy challenges*, Task Force Report, Centre for European Policy Studies - CEPS, Brussels. https://cdn.ceps.eu/wp-content/uploads/2023/12/CEPS-TFR-Quantum-Technologies-and-Cybersecurity.pdf

Shafique, M. A., Munir, A., & Latif, I. (2024). Quantum Computing: Circuits, Algorithms, and Applications. *IEEE access: practical innovations, open solutions*, *12*, 22296–22314. https://doi.org/10.1109/access.2024.3362955

Shankland, S. (2020).*Quantum computer makers like their odds for big progress*. CNET. https://www.cnet.com/tech/computing/quantum-computer-makers-like-their-odds-for-big-progress-soon/

Tan, T. G., Zhou, J., Sharma, V., & Mohanty, S. P. (2023). Post-quantum adversarial modeling: A user's perspective. *IEEE Computer*, *56*(8), 58–67. https://doi.org/10.1109/mc.2022.3218046

Vermeer, M., & Peet, E. (2020). *Securing communications in the quantum computing age: Managing the risks to encryption*. RAND Corporation. https://doi.org/10.7249/rr3102

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*