OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

Gobernanza cuántica para la seguridad de la información en el contexto universitario venezolano

Quantum governance for information security in the Venezuelan university context

Edward Arévalo
Universidad Dr. Rafael Belloso Chacín (URBE)
ORCID: https://orcid.org/0009-0005-3842-9931
edjarevalo@gmail.com
Falcón-Venezuela

Resumen

El artículo destaca la importancia de garantizar la seguridad de la información en el contexto de las instituciones universitarias venezolanas, abordando los múltiples desafíos tecnológicos, económicos, sociales, éticos y legales que dificultan la protección de la confidencialidad, integridad y disponibilidad de los datos sensibles. En respuesta a estos retos, se propone un constructo teórico sobre gobernanza cuántica basado en una metodología holística que incorpora diversas perspectivas teóricas, epistemológicas, axiológicas, filosóficas, ontológicas y sociológicas. La investigación empleó la metodología de Bagozzi y Phillips (1982), reconocida por su capacidad para integrar constructos teóricos en modelos coherentes y aplicables. Este enfoque resulta especialmente adecuado para afrontar la complejidad del sector universitario, donde interactúan diversas variables y actores. Entre los elementos fundamentales identificados se encuentran la estructura organizacional, las políticas y procedimientos, la gestión de riesgos, y los programas de concientización y capacitación en seguridad de la información. Asimismo, se subraya la importancia de las capacidades institucionales, incluyendo el acceso a recursos y conocimientos especializados, como factores críticos para la implementación exitosa. El marco de gobernanza cuántica planteado no solo proporciona soluciones adaptativas y robustas, sino que también promueve un entorno seguro y confiable para la comunidad universitaria. Este enfoque integral permite abordar los desafíos dinámicos y emergentes en materia de seguridad de la información, posicionando a las universidades como líderes en la transformación digital y la resiliencia frente a amenazas tecnológicas complejas atribuidas a la supremacía cuántica.

Palabras clave:

Gobernanza cuántica; seguridad de la información; universidades venezolanas; criptografía cuántica; supremacía cuántica

Abstract

The article highlights the importance of ensuring information security in the context of Venezuelan university institutions, addressing the multiple technological, economic, social, ethical, and legal challenges that hinder the protection of the confidentiality, integrity, and availability of sensitive data. In response to these challenges, a theoretical construct of quantum governance is proposed, based on a holistic methodology that incorporates various theoretical, epistemological, axiological, philosophical, ontological, and sociological perspectives. The research employed the methodology of Bagozzi and Phillips (1982), recognized for its ability to integrate theoretical constructs into coherent and applicable models. This approach is particularly suitable for addressing the complexity of the university sector, where diverse variables and actors interact. Among the key elements identified are organizational structure, policies and procedures, risk management, and awareness and training programs on information security. Additionally, the importance of institutional capabilities, including access to resources and specialized knowledge, is emphasized as critical factors for successful implementation. The proposed quantum governance framework not only provides adaptive and robust solutions but also promotes a secure and trustworthy environment for the university community. This comprehensive approach enables the addressing of dynamic and emerging challenges in information security, positioning universities as leaders in digital transformation and resilience against complex technological threats attributed to quantum supremacy.

Keywords:

Quantum governance; information security; venezuelan universities; quantum cryptography; quantum supremacy

OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

Introducción

La seguridad de la información en instituciones universitarias constituye un eje central dentro de la gobernanza digital, especialmente en el contexto venezolano, donde factores económicos y tecnológicos generan desafíos en la protección de datos sensibles. En este estudio, se propone un constructo teórico sobre gobernanza cuántica que incorpora principios de la computación y la criptografía cuánticas como mecanismos de protección y resiliencia ante amenazas emergentes. La gobernanza cuántica permite la formulación de modelos adaptativos, en los cuales los sistemas de seguridad pueden responder de manera dinámica y distribuida a los riesgos asociados con la supremacía cuántica y la obsolescencia de los protocolos criptográficos tradicionales (Shor, 1994).

Desde el punto de vista metodológico, la propuesta se fundamenta en el enfoque holístico de Bagozzi y Phillips (1982), integrando aspectos estratégicos, filosóficos y sociológicos para la conceptualización del constructo de seguridad cuántica. En términos de estrategia competitiva, se asumen los principios de Porter (1980), resaltando la necesidad de adaptación continua en un entorno de seguridad en evolución. Asimismo, se incorpora el análisis de la competencia en ciberseguridad propuesto por Davenport (1993), el cual enfatiza la importancia de la gestión del conocimiento en la defensa ante ataques cuánticos. En cuanto a la disrupción tecnológica, Moore (1996) señala que los avances en computación cuántica requieren nuevas estructuras de gobernanza capaces de mitigar impactos adversos en la seguridad de la información.

En el ámbito epistemológico, el constructo se sustenta en la perspectiva crítica de Karl Popper (1963), estableciendo la necesidad de evaluar la falsabilidad de los protocolos de seguridad cuántica y su capacidad de adaptación en entornos universitarios. Desde una visión axiológica, se adoptan los principios éticos de Kant (1785), los cuales orientan la protección de la información bajo imperativos categóricos que garantizan la privacidad y la integridad de los datos. En cuanto al pensamiento sistémico, Prigogine (1997) aporta la noción de estructuras dinámicas en la gobernanza de la información, lo que permite la optimización de los procesos de seguridad bajo un enfoque adaptativo. A nivel ontológico, Floridi (2010) conceptualiza la información como un objeto fundamental en los sistemas digitales, lo que refuerza la importancia de su protección en el ámbito universitario. Finalmente, desde una perspectiva sociológica, Habermas (1981) analiza la participación democrática en la configuración de la gobernanza tecnológica, resaltando la necesidad de que actores académicos se involucren en la formulación de políticas de seguridad digital.

Desde la perspectiva de Porter (1980), la tecnología juega un papel crucial en determinar la posición competitiva de una organización, influyendo en la madurez tecnológica, la intensidad tecnológica y el ciclo de vida de la tecnología implementada. En el contexto universitario, estos elementos adquieren una relevancia particular cuando se integran en un constructo teórico sobre gobernanza cuántica para la seguridad de la información, dado que la computación y la criptografía cuántica modifican sustancialmente el paradigma tradicional de protección de datos implementado.

La madurez tecnológica, entendida como el grado de evolución y perfeccionamiento de las tecnologías utilizadas en las universidades, se vincula directamente con la adopción de protocolos de seguridad. La fiabilidad y eficiencia de estas tecnologías permiten reducir vulnerabilidades asociadas a sistemas criptográficos tradicionales, los cuales podrían quedar obsoletos ante la llegada de la computación cuántica (Shor, 1994). En este sentido, la implementación de criptografía poscuántica se convierte en una estrategia competitiva clave para optimizar la seguridad de la información y reducir costos operativos vinculados a brechas de seguridad.

Desde la óptica de la intensidad tecnológica, la dependencia de los sistemas universitarios respecto a la infraestructura digital exige una transición hacia modelos de seguridad cuántica que garanticen la confidencialidad,

Depósito legal: PP201402DC4456
ISSN: 2343-6212

integridad y disponibilidad de los datos. La inversión en investigación y desarrollo (I+D), junto con la adopción de tecnologías cuánticas avanzadas, facilita la protección de redes universitarias contra ciberataques sofisticados, como los que podrían ejecutarse mediante algoritmos cuánticos de factorización (Bernstein, *et al*., 2009). La gobernanza cuántica, en este sentido, establece protocolos dinámicos capaces de adaptarse al principio de incertidumbre tecnológica, permitiendo una respuesta proactiva ante riesgos emergentes.

En términos del ciclo de vida tecnológico, la computación cuántica redefine las etapas de introducción, crecimiento, madurez y declive de las tecnologías de seguridad, acelerando la obsolescencia de sistemas tradicionales y requiriendo una gobernanza adaptativa. En el contexto universitario venezolano, la mitigación de la obsolescencia programada es fundamental para preservar la operatividad de los procesos académicos y administrativos. Es por ello, que modelos de seguridad cuántica basados en supremacía cuántica y resiliencia digital permiten garantizar la continuidad operativa de las universidades, asegurando la confidencialidad e integridad de los datos en entornos educativos altamente dinámicos (NIST, 2023). Por lo tanto, resulta vital la conceptualización de un constructo que genere los cimientos para operacionalizar la infraestructura tecnológica implementada.

Este constructo teórico sobre gobernanza cuántica para la seguridad de la información proporciona un marco multidimensional que integra los principios competitivos de Porter (1980), con estrategias de seguridad basadas en la computación cuántica, generando un modelo de protección robusto frente a los desafíos del futuro digital. Su implementación permitirá no solo optimizar los procesos internos de las universidades, sino también fortalecer su posición estratégica en el ecosistema global de educación superior.

Tomando como referencia a Davenport (1993), particularmente en su trabajo sobre estrategias competitivas, la cultura organizacional se establece como un componente esencial dentro de la gobernanza cuántica para la seguridad de la información en instituciones universitarias. En este constructo teórico, los valores, creencias y prácticas compartidas en la gestión de seguridad se redefinen bajo un esquema que incorpora los principios de la computación cuántica, permitiendo una adaptación más resiliente a las amenazas emergentes.

La seguridad cuántica exige una transformación cultural organizacional, en la cual la comunidad universitaria debe interiorizar la necesidad de enfoques dinámicos y no deterministas en la protección de datos. Esto implica una transición desde modelos tradicionales de seguridad hacia sistemas basados en superposición y entrelazamiento cuántico, los cuales permiten asegurar la confidencialidad e integridad de la información mediante la distribución cuántica de claves (Bennett y Brassard, 1984). Esta adaptación también fomenta la innovación tecnológica, permitiendo a las universidades venezolanas desarrollar esquemas de seguridad capaces de anticipar posibles vulnerabilidades antes de que sean explotadas por adversarios con capacidades computacionales avanzadas.

Por otra parte, la estructura organizacional resulta un pilar fundamental en la formulación de un constructo de gobernanza cuántica, ya que define cómo se distribuyen, coordinan y supervisan los recursos en la gestión de seguridad de la información. Una estructura flexible y escalable es indispensable para responder de manera rápida y eficiente a los desafíos impuestos por la computación cuántica. Modelos tradicionales de gestión centralizada pueden resultar insuficientes en este nuevo paradigma, por lo que la adopción de sistemas distribuidos de seguridad cuántica basados en computación en la nube y protocolos cuánticos se vuelve crucial para operacionalizar los procesos (Pirandola, *et al*., 2020).

Además, la gobernanza cuántica incorpora el aprendizaje y la mejora continua, permitiendo a las universidades actualizar sus estrategias de seguridad conforme avanza la tecnología cuántica. Esto implica que los mecanismos de protección deben ser diseñados no solo para resistir ataques actuales, sino también para ser adaptables a futuras innovaciones en algoritmos cuánticos y desarrollo de *hardware* cuántico (Shor, 1994). En este sentido, el modelo

OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

de seguridad no solo debe alinearse con estándares internacionales de criptografía poscuántica, como los recomendados por el NIST (2023), sino también con enfoques filosóficos y epistemológicos que aseguren su sostenibilidad en el tiempo.

Desde la perspectiva de Moore (1996), particularmente en su obra *Crossing the Chasm*, el análisis del entorno organizacional a través de las dimensiones; competitiva, regulatoria y social resulta clave para comprender la transición hacia la gobernanza cuántica para la seguridad de la información en universidades. Este constructo teórico aprovecha los principios de la computación cuántica para redefinir la manera en que las instituciones académicas gestionan sus riesgos y protegen sus datos, integrando dinámicamente los factores que afectan su operación en el entorno universitario.

En cuanto al entorno competitivo, las universidades deben enfrentar retos tecnológicos derivados de la supremacía cuántica y la obsolescencia de los sistemas tradicionales de seguridad (Shor, 1994). La criptografía poscuántica, propuesta por Bernstein, *et al*., (2009), representa una solución estratégica para mantener ventajas competitivas en la protección de datos sensibles, evitando que actores externos exploten vulnerabilidades provocadas por la computación cuántica. Asimismo, la adopción de tecnología cuántica en ciberseguridad se convierte en un diferenciador clave dentro del ecosistema universitario, permitiendo a las instituciones optimizar la eficiencia de sus sistemas de protección.

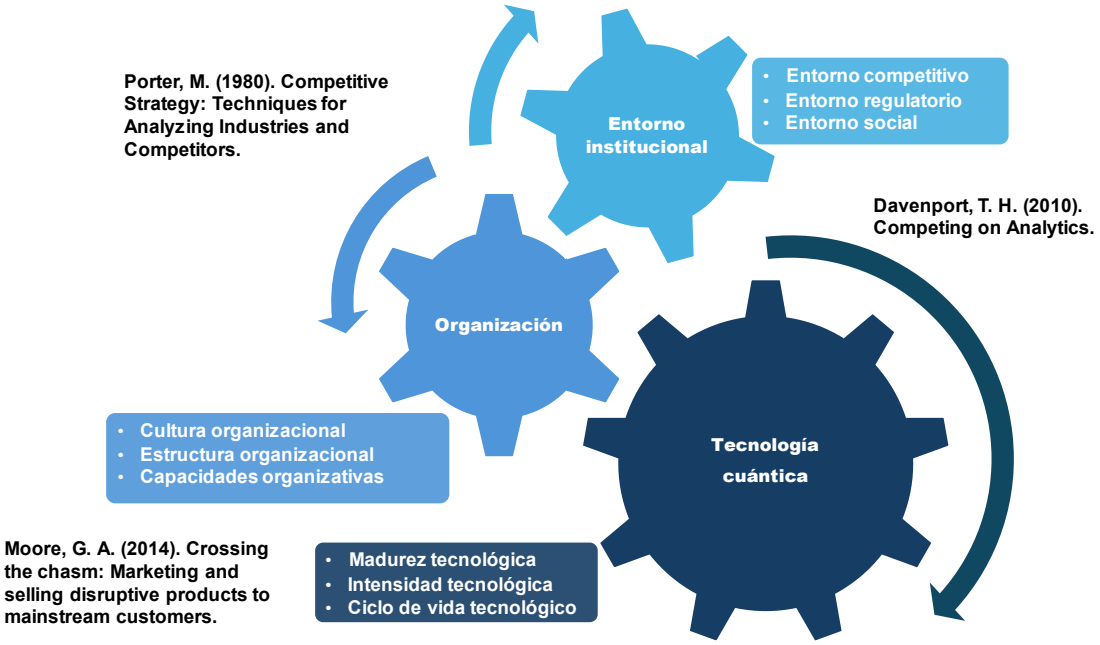
Desde la perspectiva del entorno regulatorio, la gobernanza cuántica debe alinearse con las normas gubernamentales y los estándares internacionales en materia de seguridad de la información. Organismos como el NIST (2023) han establecido procesos de estandarización para la criptografía poscuántica, lo que obliga a las universidades actualizar sus políticas de protección y resiliencia ante futuros ataques cuánticos. En el caso venezolano, la integración de regulaciones sobre gestión tecnológica y protección de datos universitarios debe contemplar mecanismos adaptativos que permitan la validación cuántica de identidades digitales y la seguridad en la transferencia de información académica.

Por último, el entorno social juega un papel esencial en la gobernanza cuántica, ya que la comunidad universitaria debe comprender y adoptar estos nuevos paradigmas de seguridad. Floridi (2010) argumenta que la ontología de la información es fundamental en la era digital y con mayor influencia será en la era cuántica, por lo que la gobernanza cuántica no solo debe enfocarse en la tecnología, sino también en la concientización y la educación sobre el impacto de la computación cuántica en la seguridad de los datos. En este sentido, estrategias de integración social, basadas en los modelos participativos propuestos por Habermas (1981), pueden fortalecer la aceptación y el desarrollo de sistemas de protección, avanzados en el ámbito universitario.

La contextualización del objeto de estudio, dentro de un constructo teórico sobre gobernanza cuántica, para la seguridad de la información se alinea con una lógica interdisciplinaria que integra la organización, la tecnología y el entorno institucional (ver Figura Nº 1).

Depósito legal: PP201402DC4456
ISSN: 2343-6212

Figura N° 1. Contextualización inherente a las variables



Fuente: Elaboración propia (2025).

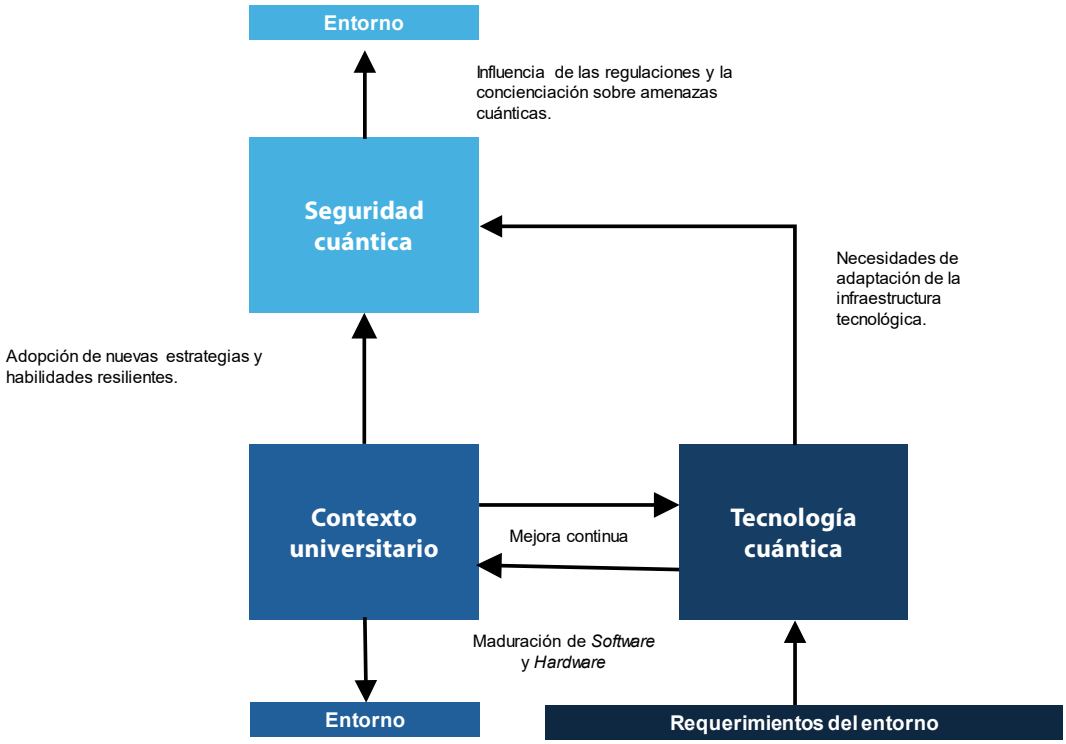
Desde el marco de un constructo teórico sobre gobernanza cuántica, para la seguridad de la información, se deben integrar los principios fundamentales de la computación y criptografía cuántica, con el fin de fortalecer la protección de los datos ante amenazas emergentes. La implementación de los protocolos de seguridad cuántica permitirá a las instituciones educativas responder de manera proactiva a los riesgos derivados de la supremacía cuántica, asegurando la confidencialidad, integridad y disponibilidad de la información académica y administrativa.

Asimismo, la gobernanza cuántica optimiza el uso de recursos limitados mediante esquemas de seguridad adaptativos que reducen costos operativos en protección digital y favorecen la sostenibilidad de la infraestructura universitaria (NIST, 2023). En el aspecto normativo, la adopción de estándares internacionales de seguridad cuántica permite a las universidades cumplir con las regulaciones, evitando brechas legales y fortaleciendo su resiliencia digital.

La seguridad de la información cuántica debe basarse en un proceso continuo de evaluación y mejora, siguiendo el principio de falsación de Popper establecidos por Barroso (2016). Esto permite a las universidades adaptar sus políticas y procedimientos según las nuevas amenazas, riesgos, vulnerabilidades y avances tecnológicos, manteniendo un estado de preparación constante que permita mitigar posibles efectos directos o colaterales, que afecten la confidencialidad, integridad y disponibilidad de los procesos y los datos. En tal sentido, existe una estrecha relación entre la seguridad cuántica, la tecnología cuántica y el contexto universitario, los cuales se encuentran sujetos al entorno y sus requerimientos cambiantes; así mismo, son influenciados por las regulaciones y la concientización sobre amenazas cuánticas, como también con las necesidades de adaptación de la infraestructura tecnológica por la adopción de nuevas estrategias y habilidades resilientes. Tal cual, como se puede evidenciar en la Figura Nº 2:

OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

Figura N° 2. Sistematización de la gestión de la seguridad cuántica



Fuente: Elaboración propia (2025).

En vista de ello, la sistematización de la gestión de la seguridad cuántica se basa en un ciclo de mejora continua que permite la adaptación progresiva de políticas y tecnologías en el contexto universitario venezolano. La evaluación constante de riesgos, siguiendo el principio de falsación de Popper, garantiza que los protocolos de seguridad cuántica evolucionen conforme aparecen nuevas amenazas, reduciendo vulnerabilidades críticas.

La maduración de *software* y *hardware* dentro de este constructo teórico permite a las universidades desarrollar estrategias de seguridad sostenibles frente a la supremacía cuántica. La adopción de sistemas distribuidos y redes cuánticas garantiza una infraestructura resiliente, minimizando los efectos de la obsolescencia tecnológica (NIST, 2023). Además, la integración de estándares globales y regulaciones académicas facilita que la gobernanza cuántica se ajuste a las normativas nacionales e internacionales, optimizando la interacción entre la tecnología cuántica, el entorno institucional y las capacidades organizacionales.

Desde otra perspectiva, el constructo teórico sobre gobernanza cuántica para la seguridad de la información se sustenta desde la ética kantiana según Malishev (2014), ya que integra el respeto a la privacidad y los derechos individuales en entornos académicos, investigativos y administrativos. Además, la transparencia y legitimidad institucional se refuerzan mediante procesos verificables de seguridad cuántica, alineando la gestión tecnológica con estándares éticos de confianza y equidad en la protección de la información.

Bajo el constructo teórico sobre gobernanza cuántica para la seguridad de la información, la visión de Nastidas (2011) basada en la filosofía de Prigogine resalta la necesidad de estrategias adaptativas en entornos universitarios. La seguridad cuántica, al considerar la naturaleza dinámica de las amenazas digitales, permite anticipar y responder proactivamente mediante los sistemas resilientes. La criptografía cuántica y los modelos de protección

Depósito legal: PP201402DC4456
ISSN: 2343-6212

distribuida optimizan la integridad y disponibilidad de los datos, garantizando un esquema de gobernanza flexible ante eventos imprevistos (Bernstein, *et al*., 2009).

Asimismo, un constructo teórico sobre gobernanza cuántica para la seguridad de la información es fundamental para abordar la gestión de los datos del contexto universitario por su valor intrínseco como activo digital esencial actual y su protección estructurada mediante enfoques deliberativos y participativos que generará la interacción de un ecosistema cuántico. Es por ello que, para Floridi (2012) la información debe ser gestionada con el mismo rigor que los activos tangibles críticos, lo que refuerza la necesidad de integrar mecanismos de seguridad avanzados, como la criptografía cuántica basada en la distribución segura de claves (Bennett y Brassard, 1984). Esto garantiza que la confidencialidad, integridad y disponibilidad de los datos se mantengan frente a riesgos tecnológicos emergentes.

Por otro lado, el marco de Habermas (1984), adaptado por Ibrobo (2020), sugiere que la formulación de políticas de seguridad debe ser resultado de un proceso inclusivo y transparente, donde los actores del contexto universitario participen activamente en la generación de estrategias de protección cuántica. Este enfoque participativo no solo mejora la adopción de tecnologías de seguridad, sino que fortalece la legitimidad institucional, asegurando que la gobernanza cuántica se implemente con aceptación y eficacia dentro de la comunidad educativa. La seguridad cuántica, al incorporar principios de deliberación democrática, favorece un entorno académico, investigativo y administrativo donde la protección de los datos no solo responde a exigencias tecnológicas, sino también a principios éticos y sociales que regulan el ecosistema universitario.

En referencia de ello, resulta fundamental la conceptualización del estado actual de la seguridad de la información en el contexto universitario venezolano que se enfoque en la sistematización de los siguientes aspectos:

- Identificación de políticas y procedimientos que integran la criptografía poscuántica y mecanismos de validación cuántica para garantizar la protección del entorno tangible e intangible.

- Evaluación de la madurez de los marcos de gobernanza mediante el análisis exhaustivo de la capacidad institucionales para adoptar estándares de seguridad cuántica con estrategias de resiliencia operativa que garantice una transición eficiente hacia modelos capaces de mitigar riesgos y resistir ataques cuánticos.

- Análisis de brechas bajo un enfoque multidimensional que incorpore principios de computación cuántica, gobernanza flexible y seguridad adaptativa, permitiendo al contexto universitario venezolano fortalecer su resiliencia frente a la supremacía cuántica.

Para establecer los atributos clave de un constructo teórico sobre gobernanza cuántica en la gestión de la seguridad de la información, es fundamental analizar las diversas dimensiones que incluyen aspectos técnicos, organizacionales y humanos. Estas dimensiones deben integrarse de manera coherente con los elementos conceptuales y operativos, asegurando su alineación con los requerimientos presentes y futuro; ya que la gobernanza cuántica debe ser flexible y adaptativa, permitiendo una evolución constante ante cambios tecnológicos y las nuevas amenazas en contextos intangibles.

Para ello, se consideran los siguientes aspectos:

a) La estructura organizacional debe integrar principios de seguridad cuántica para garantizar una gestión resiliente y adaptativa en entornos universitarios, en función de:

- Roles y responsabilidades: la designación de un CISO (*Chief Information Security Officer*) y comités de seguridad debe considerar la implementación de protocolos cuánticos de protección, asegurando que la gestión de riesgos se fortalezca ante amenazas computacionales avanzadas.

- Jerarquía y coordinación: la gobernanza cuántica requiere una estructura flexible y escalable, facilitando la interacción entre unidades de trabajo mediante sistemas de distribución cuántica de claves que optimicen la seguridad de la información.

Depósito legal: PP201402DC4456
ISSN: 2343-6212

OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

• Comunicaciones internas: la implementación de criptografía cuántica en la transmisión de información garantiza la integridad y confidencialidad de los datos en todos los niveles institucionales, promoviendo una gobernanza más segura y eficiente.

b) Las políticas y procedimientos deben alinearse con principios de criptografía cuántica y protección adaptativa frente a amenazas emergentes, considerando los siguientes aspectos:

• Normativas claras y actualizadas: la gobernanza cuántica exige regulaciones dinámicas, ajustadas a los avances de la computación cuántica y la evolución de riesgos en entornos intangibles.

• Procedimientos detallados: la gestión de incidentes debe incorporar protocolos poscuánticos y modelos de validación cuántica para garantizar la seguridad de accesos y datos sensibles.

• Revisión y mejora continua: la formulación de políticas debe adaptarse a la supremacía cuántica mediante auditorías periódicas y estrategias resilientes que aseguren la efectividad de los mecanismos de protección.

c) La gestión de riesgos debe basarse en enfoques dinámicos que incorporen criptografía cuántica y técnicas predictivas avanzadas para identificar y reducir vulnerabilidades en entornos tangibles e intangibles en evolución, bajo las siguientes consideraciones:

• Identificación de riesgos: la seguridad cuántica debe optimizar la identificación de riesgos mediante el uso de métodos avanzados que detecten amenazas en tiempo real como un mecanismo preventivo, garantizando la integridad y protección de la información frente a posibles vulnerabilidades.

• Evaluación de riesgos: la gobernanza cuántica debe orientarse en un análisis dinámico que determine con precisión las probabilidades de ataque y la capacidad de resistencia frente a algoritmos de factorización cuántica mediante protocolos adaptativos y estrategias criptográficas poscuánticas.

• Planes de mitigación: la gobernanza cuántica debe desarrollar estrategias de resiliencia activa, asegurando que los protocolos poscuánticos fortalezcan la protección de la infraestructura del contexto universitario frente a la supremacía cuántica que amenaza el entorno tecnológico por las prácticas de acciones reactivas.

d) La concientización y capacitación deben alinearse con las necesidades actuales y futuras del contexto universitario, garantizando la preparación ante amenazas emergentes y la adaptación tecnológica requerida orientada en el usuario como el eslabón más débil de la cadena de custodia cuántica. Para ello, es necesario contemplar aspectos como:

• Programas de formación: la seguridad cuántica debe alinearse en la formulación de programas de capacitación continua que tomen en consideración la necesidad de una alfabetización digital cuántica, donde estudiantes, docentes, investigadores y personal administrativo adquieran habilidades para gestionar riesgos poscuánticos y aplicar protocolos de protección avanzados.

• Sensibilización del personal: la seguridad cuántica debe enfocarse en campañas de sensibilización que promuevan una cultura de seguridad cuántica, asegurando que todos los miembros de la organización comprendan las amenazas que la supremacía cuántica representa para la protección de la información y la continuidad de operativo de los procesos inherentes a la comunidad universitaria.

• Evaluación de la capacitación: la seguridad cuántica debe orientarse en el establecimiento de mecanismos que midan la efectividad de los programas de formación asociados a los riesgos inherentes a la seguridad cuántica, asegurando que los conocimientos adquiridos sean aplicables y relevantes. Este proceso debe incluir análisis permanentes, retroalimentación de los participantes y ajustes estratégicos para optimizar el contenido según las necesidades emergentes de la supremacía cuántica.

e) La infraestructura tecnológica debe evolucionar hacia un entorno resistente a ataques cuánticos asegurando la confidencialidad, integridad y disponibilidad de

Depósito legal: PP201402DC4456
ISSN: 2343-6212

los datos mediante enfoques adaptativos que consideren los siguientes elementos:

• Infraestructura segura: conceptualizada bajo la implementación de infraestructuras seguras bajo los requerimientos de seguridad cuántica que debe incorporar tecnologías avanzadas que garanticen la protección de la información frente a la supremacía cuántica. Esto implica la integración de firewalls cuánticos, capaces de detectar anomalías con modelos predictivos; sistemas de detección de intrusiones poscuánticos, que analizan el tráfico en tiempo real para prevenir ataques avanzados; y soluciones de encriptación cuántica, asegurando que los datos sensibles permanezcan protegidos mediante algoritmos de criptografía poscuántica resistentes a la computación cuántica.

• Monitoreo y detección: operacionalizada bajo herramientas de monitoreo continuo a tiempo real que deben incorporar algoritmos poscuánticos capaces de analizar grandes volúmenes de datos y detectar anomalías que respondan a los incidentes cuánticos.

• Actualización y mantenimiento: definida en base a políticas para la actualización y mantenimiento de los lineamientos establecidos en la seguridad cuántica para garantizar la protección de la información frente a las amenazas derivadas de la supremacía cuántica, tomando en consideración la criptografía poscuántica, el monitoreo proactivo de patrones cuánticos y la distribución cuántica de claves.

f) El cumplimiento y auditoría en el marco de la gobernanza cuántica de la seguridad de la información debe garantizar que las instituciones del contexto universitario venezolano se adapten a los nuevos desafíos tecnológicos, protegiendo sus sistemas frente a la supremacía cuántica. Con relación a ello, debe contemplar los siguientes aspectos:

• Cumplimiento normativo: enmarcado a regulaciones y estándares tecnológicos, como ISO/IEC 27001:2022 *Information Security, Cybersecurity and Privacy Protection*, ISO/IEC 27002:2022 *Information security controls*, ISO/IEC 27005:2022 *Information Security Risk Management*, ISO/IEC 15408-1:2022 *Common Criteria for Information Technology Security Evaluation*, NIST SP 800-207 *Zero Trust Architecture*, NIST SP 800-208 *Post-Quantum Cryptography Migration Guidelines*, Reglamento (UE) 2016/679 *General Data Protection Regulation* (GDPR), Reglamento (UE) 2022/2554 *Digital Operational Resilience Act* (DORA), Directiva (UE) 2022/2555 – NIS2 *Network and Information Security Directive*, IEEE P7130 *Standard for Quantum Computing Definitions*, IEEE P1913 *Quantum Key Distribution Security Framework*, IEEE P1913 *Quantum Key Distribution Security Framework* y E91 *Protocol Quantum Key Distribution using Entanglement*.

• Auditorías regulares: la seguridad cuántica debe armarse de procesos de auditorías internas y externas permanentes para evaluar el estado de la seguridad de la información; y asegurar el cumplimiento continuo que garantice que los sistemas de protección de la información sean resilientes ante los ataques derivados de la computación cuántica.

• Informes y documentación: cumpliendo con los lineamientos de formulación de documentación exhaustiva y precisa para garantizar la trazabilidad y actualización de políticas, procedimientos, auditorías e incidentes relacionados con la protección de la información frente a amenazas cuánticas en el contexto universitario venezolano.

g) Resiliencia organizacional: esquematizada por la capacidad de las instituciones universitarias para anticipar, resistir, responder y recuperarse de incidentes de seguridad derivados de la evolución de la computación cuántica, abordando los siguientes aspectos:

• Planes de continuidad del negocio: orientados en el desarrollo e implementación de planes que aseguren que los algoritmos y sistemas sigan operando de manera segura tras la obsolescencia de métodos criptográficos clásicos. Así como las estrategias de protección que garanticen que los accesos y recursos sean seguros frente a ataques cuánticos.

Depósito legal: PP201402DC4456
ISSN: 2343-6212

OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

• Recuperación de desastres: enmarcado en la formulación de estrategias y procedimientos para la recuperación rápida y efectiva de la información y los sistemas tras un incidente de seguridad asociados a los ataques y vulnerabilidades cuánticas.

• Pruebas y simulacros: sujeto a la ejecución de pruebas y simulacros regulares para evaluar la efectividad de los planes de continuidad y recuperación, y ajustar las estrategias según sea necesario para medir la robustez de los sistemas ante la supremacía cuántica.

Metodología

La metodología de Bagozzi y Phillips (1982) se basa en la integración de diversos constructos teóricos en un modelo coherente, lo que la hace particularmente útil para estructurar la seguridad cuántica de la información en el contexto universitario venezolano, puesto que la computación cuántica introduce nuevas amenazas y vulnerabilidades a los sistemas de seguridad implementados, lo que requiere un enfoque multidimensional capaz de modelar las interacciones entre tecnología, regulaciones, resiliencia organizacional y protección de datos.

Desde esta perspectiva, la metodología permite conceptualizar un constructo teórico sobre gobernanza cuántica, donde convergen aspectos como la criptografía poscuántica, los protocolos de distribución cuántica de claves (BB84, E91) y la gestión de riesgos cuánticos. Además, facilita la incorporación de normativas internacionales como la serie ISO/IEC 27000:2022, GDPR, NIS2 y DORA, asegurando un marco regulatorio que evolucione conforme a las necesidades de protección ante la supremacía cuántica.

En el sector universitario venezolano la convergencia de elementos esenciales, como la gestión de infraestructura digital y la protección de datos en ámbitos académicos, administrativos, investigativos y personales, demandan la aplicación de un enfoque teórico estructurado para fortalecer la capacidad de las instituciones frente a los desafíos de la seguridad cuántica. La metodología de Bagozzi y Phillips proporciona un modelo analítico integral, que permite anticipar, resistir, responder y recuperarse de incidentes de seguridad generados por la evolución de la computación cuántica, minimizando riesgos y garantizando la continuidad operativa. Este marco teórico facilita la formulación de estrategias adaptativas que optimizan la resiliencia digital, impulsando la transición hacia protocolos poscuánticos y sistemas avanzados de protección, asegurando la integridad, confidencialidad y disponibilidad de la información en un entorno académico en constante transformación y alineado con los principios de la gobernanza cuántica.

Este enfoque permite que las universidades desarrollen modelos sólidos para enfrentar los desafíos de la seguridad cuántica, garantizando la evolución de sus políticas de protección de la información abordando los siguientes aspectos:

• Construcción teórica:

a) Descomposición de los conceptos clave como gobernanza cuántica, seguridad de la información cuántica y capacidades institucionales en los subcomponentes básicos que operacionalizan los procesos inherentes.

b) Identificación de las relaciones entre estos componentes para formar una red teórica que explique cómo interactúan estos elementos para influir en la seguridad de la información cuántica.

• Validación empírica:

La validación empírica en el contexto de una investigación documental implica comprobar que los datos y teorías obtenidos a través de la revisión de documentos están respaldados por evidencias reales y verificables. Este proceso es crucial para garantizar la fiabilidad y validez de los resultados de la investigación, en referencia a:

a) Recolección de documentación:

• Artículos académicos sobre gobernanza cuántica y seguridad de la información cuántica.

• Políticas y procedimientos internos de universidades sobre seguridad de la información implementados.

Depósito legal: PP201402DC4456
ISSN: 2343-6212

b) Análisis crítico:

• Evaluación de las prácticas y políticas mencionadas en los documentos.

• Evaluación de los informes de auditoría para entender los desafíos y éxitos en la implementación de estas prácticas y políticas.

c) Comparación con datos empíricos:

• Comparación de los datos con los hallazgos documentales para verificar la coherencia y validez.

d) Validación de conceptos:

• Confirmación de que los hallazgos documentados efectivamente mejoran la determinación de los criterios asociados a la seguridad de la información cuántica en la práctica.

• Ajuste de las recomendaciones en la investigación según los datos empíricos obtenidos.

e) Resultados:

• Presentación de un informe que detalle el proceso de validación y discuta los hallazgos, destacando la importancia de ajustar las políticas basándose en datos empíricos.

Además del enfoque documental, descriptivo y exploratorio de esta investigación, se orienta en una investigación mixta combinando el método cuantitativo y cualitativo para proporcionar una comprensión más completa y robusta del fenómeno estudiado; ya que es necesario cuantificar los incidentes de gestión de la seguridad de la información con *insights* cualitativos para validar y enriquecer los hallazgos que permitan conceptualizar el constructo teórico sobre gobernanza cuántica requerido.

En el contexto del estudio, la población objetivo se enmarca en las instituciones de educación del sector público y privado en Venezuela que ofrecen programas de educación superior. Los individuos claves corresponden al personal administrativo, personal de tecnología de la información, docentes, investigadores y estudiantes que están involucrados o afectados por las políticas y prácticas de seguridad de la información en estas casas de estudio. Específicamente aplicables a la Universidad de Falcón (Udefa), Universidad Nacional Experimental Politécnica de la Fuerza Armada (Unefa) Núcleo Falcón Extensión Punto Fijo, Universidad Nacional Experimental Simón Rodríguez (Unesr) Núcleo Coro, Universidad Nacional Experimental Francisco de Miranda (Unefm) Núcleo Sabino, Universidad del Zulia Núcleo Punto Fijo.

La fase metodológica alineadas al enfoque holístico de Bagozzi y Phillips corresponde a la siguiente estructura:

a) Diagnóstico del estado actual de la gobernanza cuántica. Esto implica una evaluación exhaustiva de las prácticas actuales en el sector universitario venezolano:

• Identificación de las políticas, normas y procedimientos existentes. Puesto que resulta crucial conocer las regulaciones y directrices actuales que rigen la seguridad de la información en las universidades venezolanas.

• Análisis de la madurez de los marcos de gobernanza cuántica para evaluar su eficacia y grado de sofisticación en la gestión de elementos intangibles.

• Evaluación de las brechas actuales para detectar oportunidades de mejora en la gobernanza cuántica y la seguridad de la información.

b) Definición de los atributos clave para el modelo de gobernanza cuántica en la seguridad de la información del contexto universitario venezolano, con el objetivo de determinar sus características esenciales:

• Identificación de los riesgos, amenazas y vulnerabilidades que afectan a las universidades en el contexto de la seguridad cuántica, considerando la posible obsolescencia de sistemas criptográficos tradicionales, la exposición a ataques cuánticos y la necesidad de migración hacia criptografía poscuántica.

• Evaluación de la frecuencia y gravedad de los incidentes de seguridad para priorizar los esfuerzos de mitigación y mejorar la respuesta a futuros incidentes de supremacía cuántica.

Depósito legal: PP201402DC4456
ISSN: 2343-6212

OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

• Evaluación del impacto de los riesgos, amenazas y vulnerabilidades cuánticas para mitigar sus efectos y fortalecer la resiliencia del sistema frente a desafíos emergentes de supremacía cuántica.

c) Conceptualización de la estructura del constructo teórico sobre gobernanza cuántica para la seguridad de la información del contexto universitario venezolano:

• Recopilación de datos sobre el marco de gobernanza cuántica requerido.

• Determinación de la sostenibilidad del modelo a largo plazo mediante las siguientes consideraciones:

– Identificación de los recursos tecnológicos, humanos y financieros requeridos.

– Evaluación de la capacidad de las universidades para actualizar y mantener el sistema a lo largo del tiempo.

– Aseguramiento de que la estructura organizacional sea flexible y capaz de adaptarse a cambios en el entorno sin comprometer la seguridad de la información.

• Identificación de los principales desafíos y obstáculos para su implementación, en base a los siguientes aspectos:

– Evaluación de posibles problemas tecnológicos que representen incompatibilidad de sistemas, obsolescencia y amenazas emergentes (riesgo tecnológico).

– Análisis de las limitaciones presupuestarias y búsqueda de financiamiento adicional, si es necesario (obstáculos económicos).

– Valoración de la resistencia al cambio de los estudiantes docentes, investigadores y personal administrativo a adoptar el marco referencial de gobernanza cuántica (resistencia al cambio).

– Evaluación del cumplimiento de regulaciones nacionales e internacionales relacionadas con la protección de datos (aspectos regulatorios).

La relación de los conceptos evidenciados en el enfoque holístico con los componentes del constructo teórico sobre gobernanza cuántica está interrelacionada mediante cuatro tipos de relaciones:

a) Relaciones de sustento: conectando los componentes con teorías subyacentes en gestión de ciberseguridad cuántica bajo el cumplimento de la ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27005:2022, ISO/IEC 15408-1:2022, NIST SP 800-207, NIST SP 800-208, Reglamento (UE) 2016/679, Reglamento (UE) 2022/2554, Directiva (UE) 2022/2555, IEEE P7130, IEEE P1913 E91.

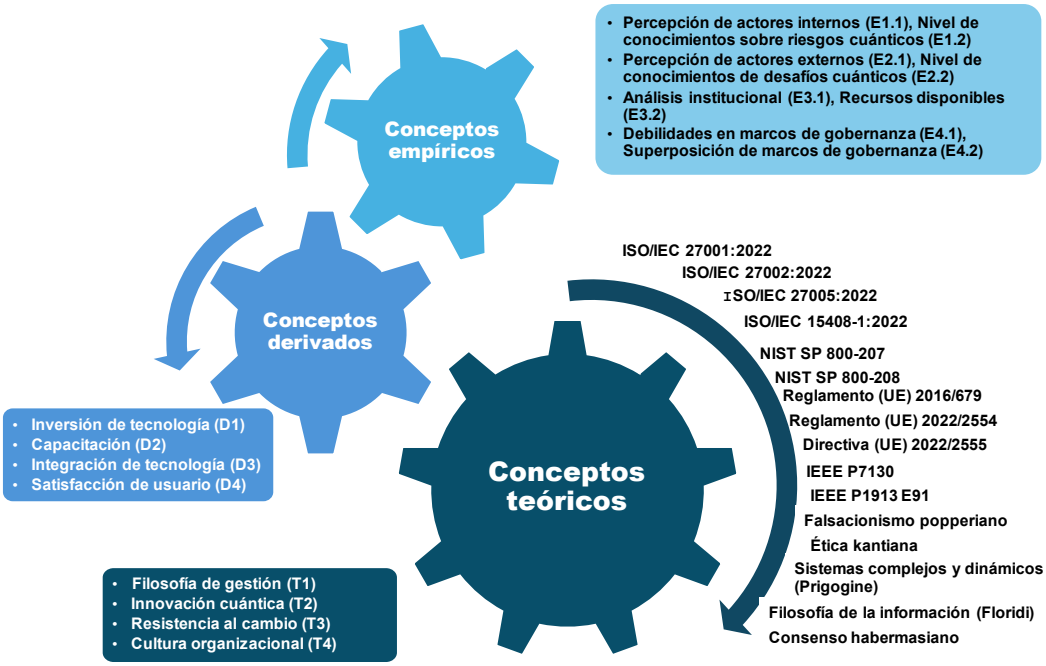
b) Relaciones de observación: analizando los componentes utilizando datos empíricos de estudios en el contexto universitario venezolano.

c) Relaciones de derivación: derivando nuevos conceptos o mejoras a partir de la aplicación práctica, como la incorporación de tecnologías emergentes para mitigar el efecto de la supremacía cuántica.

d) Relaciones de correspondencia: estableciendo correspondencias entre los conceptos teóricos (marco de referencia de gobernanza cuántica) y los datos empíricos recolectados en el entorno universitario.

Depósito legal: PP201402DC4456
ISSN: 2343-6212

Figura N° 3. Conceptos en el enfoque holístico



Fuente: Elaboración propia (2025).

A continuación, se detalla la relación de conceptos mencionada:

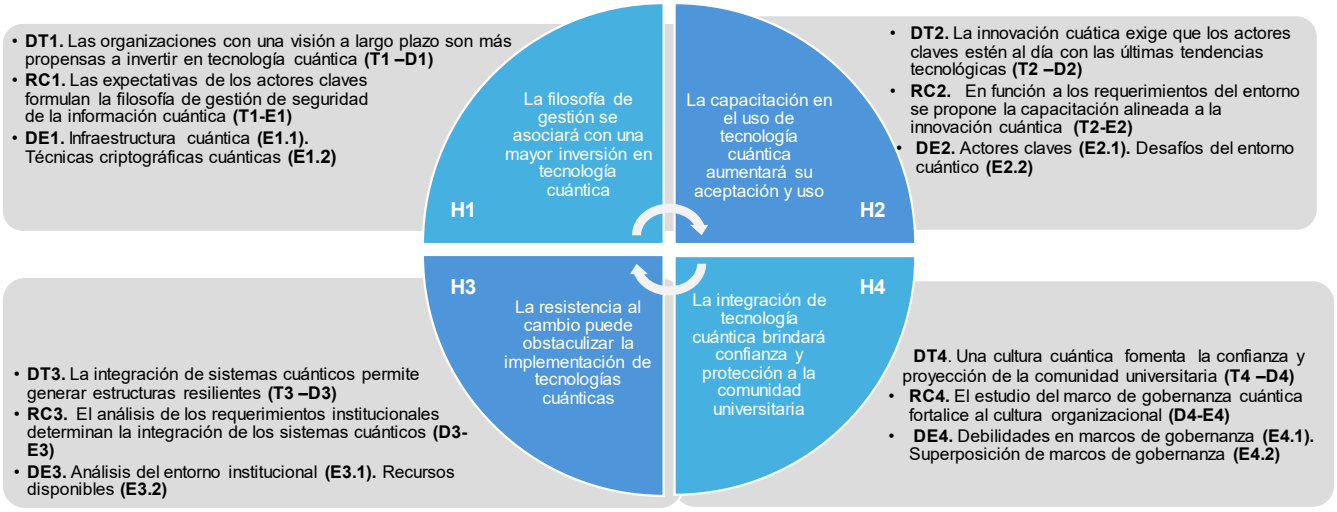
Al relacionar el enfoque holístico con un constructo teórico sobre gobernanza cuántica, es posible establecer vínculos entre los principios fundamentales de la seguridad de la información y las capacidades avanzadas que ofrece la tecnología cuántica, en especial en el ámbito de la toma de decisiones y la gestión de riesgos complejos.

El constructo teórico sobre gobernanza cuántica puede definirse como un marco interdisciplinario que incorpora conceptos de computación cuántica, criptografía poscuántica y dinámicas organizacionales. Su objetivo principal es anticipar y gestionar riesgos altamente complejos, aprovechando las propiedades únicas de los sistemas cuánticos, como la superposición y el entrelazamiento, para optimizar la toma de decisiones.

En concordancia con lo anteriormente expuesto, se presentan las relaciones del enfoque holístico con los conceptos teóricos, conceptos derivados, conceptos empíricos, reglas de correspondencia e hipótesis formuladas:

OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

Figura N° 4. Relaciones del enfoque holístico



Fuente: Elaboración propia (2025).

La conceptualización de la estructura de un constructo teórico sobre gobernanza cuántica en la seguridad de la información del contexto universitario venezolano se abordó bajo las siguientes hipótesis:

• Hipótesis 1: la filosofía de gestión se asociará con una mayor inversión en tecnología cuántica.

• Hipótesis 2: la capacitación en el uso de tecnología cuántica aumentará su aceptación y uso.

• Hipótesis 3: la resistencia al cambio puede obstaculizar la implementación de tecnologías cuánticas.

• Hipótesis 4: la integración de tecnología cuántica brindará confianza y protección a la comunidad universitaria.

En función del objeto de estudio y tomando como referencia el contexto de las universidades y la comunidad académica, la investigación se orientó en la Hipótesis 4; en donde, se asocia un constructo teórico sobre gobernanza cuántica para la seguridad de la información como factor crucial para asegurar la confidencialidad, integridad y disponibilidad de los activos tangibles e intangibles bajo las siguientes premisas:

• Protección de datos personales: para asegurar que los datos de los estudiantes, docentes, investigadores, personal administrativo estén protegidos mediante políticas robustas de privacidad y seguridad de la información.

• Ciberseguridad: para implementar sistemas y protocolos de ciberseguridad que prevengan y respondan a amenazas y ataques cibernéticos, protegiendo tanto la infraestructura tecnológica como la información almacenada.

• Formación y concienciación: para proveer la formación continua a estudiantes, docentes, investigadores y personal administrativo sobre buenas prácticas de seguridad cuántica y manejo seguro de la información.

• Políticas de uso de tecnología cuántica: para establecer políticas claras sobre el uso de dispositivos y redes en la universidad, garantizando que se utilicen de manera segura y responsable.

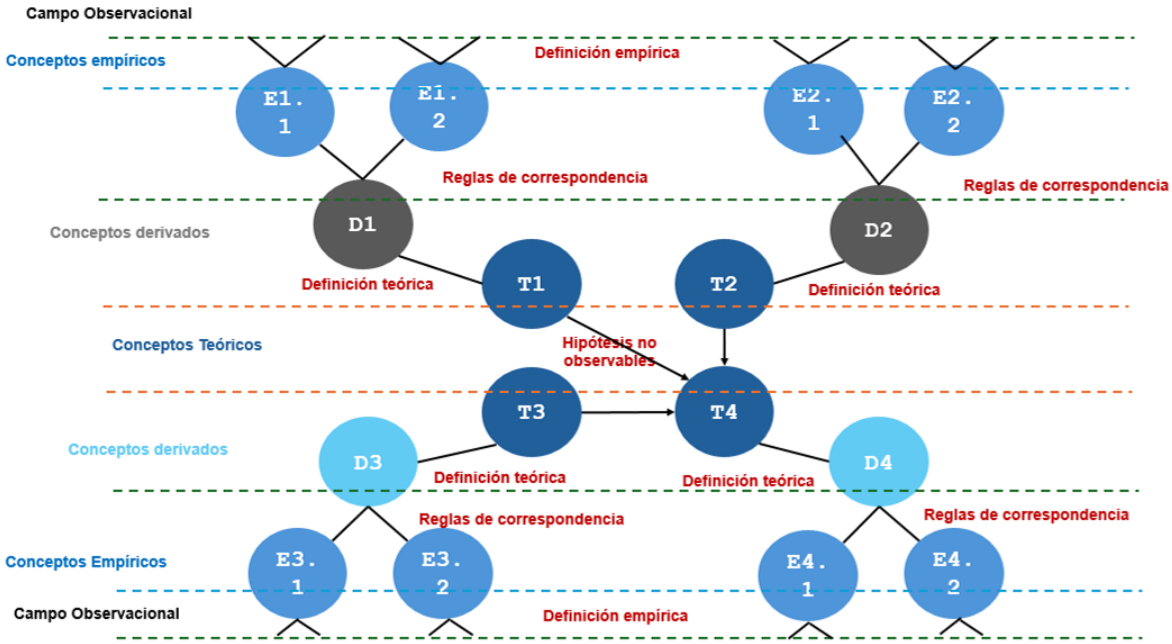
• Infraestructura segura: para asegurar que la infraestructura tecnológica, incluyendo servidores y redes, sea robusta y esté constantemente actualizada para enfrentar nuevas amenazas.

• Cumplimiento normativo: para generar un marco de gobernanza cuántica que supervise y gestione la seguridad de la información, asegurando que se cumplan con todas las normativas legales y estándares internacionales.

Depósito legal: PP201402DC4456
ISSN: 2343-6212

A continuación, se detalla la malla teórica relacional bajo la hipótesis 4 formulada, definida como: la integración de tecnología cuántica brindará confianza y protección a la comunidad universitaria.

Figura N° 5. Malla teórica relacional



Fuente: Elaboración propia (2025).

La seguridad cuántica en el contexto universitario venezolano representa un enfoque estratégico para garantizar la protección de datos y la confianza institucional. Al integrar tecnologías cuánticas, como la criptografía poscuántica, las instituciones universitarias pueden blindar la confidencialidad, integridad y disponibilidad de la información. Esto es particularmente relevante en el manejo de expedientes académicos, investigaciones científicas y datos administrativos, donde los riesgos asociados a tecnologías emergentes están en constante evolución. De esta manera, se genera un entorno seguro en el que la comunidad universitaria se sienten respaldada.

Además, la aplicación de sistemas cuánticos no solo se limita a la protección de datos, sino que también ofrece oportunidades para optimizar procesos administrativos y académicos. La capacidad de analizar grandes volúmenes de información de forma segura y eficiente permite mejorar la toma de decisiones, facilitando así la implementación de estrategias institucionales más dinámicas y adaptativas. Esto fomenta un entorno universitario resiliente, donde los participantes pueden centrarse en sus actividades sin preocupaciones por la seguridad de la infraestructura tecnológica.

El enfoque integral de la seguridad cuántica conecta la satisfacción de los usuarios de la comunidad universitaria con la resiliencia tecnológica, asegurando que la innovación y la seguridad estén alineadas con los objetivos estratégicos de las instituciones. A través de un marco robusto de gobernanza cuántica, las organizaciones universitarias pueden posicionarse como líderes en la transformación digital, respondiendo eficazmente a los desafíos de un entorno cada vez más interconectado y complejo. Este constructo teórico no solo refuerza la protección de datos, sino que también impulsa la excelencia operativa y académica.

OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

Resultados

La metodología de Bagozzi y Phillips permitió identificar varios elementos del constructo teórico que inciden directamente sobre el objeto de estudio, los cuales se encuentran definidos por las siguientes variables con su descripción asociada:

• Constructo teórico sobre gobernanza cuántica (variable independiente):

• Estructura organizacional: la estructura organizacional debe incluir roles y responsabilidades claramente definidos para la gestión de la seguridad de la información cuántica para facilitar la coordinación y comunicación entre diferentes niveles.

• Políticas y procedimientos: las políticas y procedimientos deben ser claros y comprensibles y deben integrarse con las tecnologías cuánticas disponibles para ser efectivamente implementados. En un entorno de recursos limitados, como el venezolano, las políticas deben ser pragmáticas y enfocarse en las áreas de mayor riesgo. Es crucial, que estas políticas sean comunicadas y aplicadas consistentemente en toda la universidad.

• Gestión de riesgos: la gestión de riesgos cuánticos requiere la identificación, evaluación y mitigación de riesgos tecnológicos. En un entorno incierto, como el de las universidades venezolanas, esta gestión debe ser proactiva y flexible, adaptándose rápidamente a nuevas amenazas; por lo tanto, deben abordarse los riesgos desde diferentes ángulos y proponer soluciones innovadoras.

• Concientización y capacitación: la concientización y capacitación en seguridad de la información cuántica son fundamentales para crear una cultura organizacional de seguridad. Tecnológicamente, esto incluye el uso de plataformas de *e-learning* y simulaciones de ataques para entrenar al personal de forma continua.

• Capacidades institucionales (variable mediadora):

• Conocimientos: el nivel de conocimientos en seguridad de la información cuántica depende de la capacitación y la actualización continua del personal. En el entorno venezolano, esto puede implicar alianzas con instituciones internacionales para acceder a materiales y certificaciones de las últimas tendencias en seguridad.

• Recursos: la disponibilidad de recursos financieros y tecnológicos es crucial para la implementación de medidas de seguridad cuánticas. Tecnológicamente, las universidades deben invertir en infraestructura adecuada poscuántica que mitigue el efecto de la supremacía cuántica.

• Seguridad de la Información (variable dependiente):

• Confidencialidad: En el contexto tecnológico, la confidencialidad implica el uso de herramientas de encriptación y autenticación para proteger los datos. En el entorno universitario venezolano, donde la conectividad y el acceso a tecnología avanzada pueden ser limitados, es crucial adaptar estas tecnologías a los recursos disponibles con políticas estrictas.

• Integridad: tecnológicamente, mantener la integridad de la información requiere sistemas robustos de respaldo y recuperación de datos. En un entorno con desafíos económicos como el venezolano, es vital contar con soluciones de bajo costo, pero efectivas, asegurando que cualquier cambio en la información sea autorizado y registrado.

• Disponibilidad: la disponibilidad de la información depende de la infraestructura tecnológica y su mantenimiento. En el entorno venezolano, donde las interrupciones de energía y conectividad son comunes, las universidades deben tener planes de contingencia y soluciones alternativas para asegurar el acceso continuo a la información.

Conclusión

El constructo teórico sobre gobernanza cuántica propuesto, integra diversos constructos teóricos y filosóficos, ofreciendo una visión holística y adaptable para la gestión de la seguridad de la información en entornos universita-

Depósito legal: PP201402DC4456
ISSN: 2343-6212

rios. El falsacionismo popperiano resulta crucial para definir que la seguridad de la información cuántica no es un estado estático, sino un proceso continuo de aprendizaje y adaptación. Por lo tanto, las políticas y procedimientos deben ser sometidos a pruebas constantes, revisados y actualizados en respuesta a las nuevas amenazas y vulnerabilidades inducida por la supremacía cuántica. De igual forma la ética kantiana induce que los elementos inherentes a la seguridad de la información cuántica deben ir de la mano con el respeto a los derechos y la privacidad de los usuarios de la comunidad universitaria.

En el mismo orden de ideas, la complejidad de Prigogine define que las universidades son sistemas complejos y dinámicos, donde los riesgos cuánticos emergen de interacciones no lineales. Lo que requiere una conceptualización de la gestión de riesgos flexible y adaptable para responder a eventos imprevistos y a la constante evolución del entorno tecnológico.

Asimismo, la gobernanza cuántica debe reconocer su centralidad y garantizar su integridad, disponibilidad y confidencialidad. En vista de ello, la ontología de la información de Floridi determina la información como un activo estratégico de gran valor; en el cual el consenso Habermasiano establece que las políticas de seguridad deben ser construidas a través de procesos de diálogo y consenso, involucrando a todos los actores de la comunidad universitaria para fortalecer la legitimidad y la efectividad de las medidas implementadas.

Al integrar estos elementos, el constructo propuesto ofrece una base sólida para la generación de un entorno seguro y confiable en el contexto universitario. Este enfoque integral y evolutivo permite a las instituciones educativas proteger sus activos informáticos, garantizar la privacidad de los datos y fomentar la confianza de la comunidad universitaria.

Recomendaciones

Es importante señalar que los aspectos abordados en este estudio poseen una alta aplicabilidad en diversos sectores, tanto gubernamentales como privados. Los elementos del constructo teórico sobre gobernanza cuántica propuesto trascienden el ámbito universitario, ofreciendo un enfoque integral y flexible para gestionar la seguridad de la información en diferentes contextos organizativos, especialmente frente a los desafíos y amenazas derivados del impacto de la supremacía cuántica. En vista de ello, se recomiendan las siguientes consideraciones:

- Fortalecer la estructura organizacional: es fundamental definir roles y responsabilidades claros, como la designación de un CISO (*Chief Information Security Officer*) y comités de seguridad que implementen protocolos cuánticos de protección para asegurar una gestión de riesgos más robusta y eficiente ante amenazas de la supremacía cuántica.

- Actualizar políticas y procedimientos: las normativas deben ser dinámicas y ajustadas a los avances de la computación cuántica para gestionar incidentes que afectan la confidencialidad, la integridad y la disponibilidad de la infraestructura tecnológica y los servicios implementados.

- Invertir en infraestructura tecnológica: la implementación de tecnologías avanzadas como *firewalls* cuánticos, sistemas de detección de intrusiones poscuánticos y soluciones de encriptación cuántica es esencial para proteger la información frente a la supremacía cuántica.

- Promover la concientización y capacitación: la formación continua en seguridad cuántica es crucial para que todos los miembros de la organización comprendan las amenazas y adopten buenas prácticas de protección acordes a la supremacía cuántica.

- Realizar auditorías regulares: es importante llevar a cabo auditorías internas y externas periódicas para evaluar el estado de la seguridad de la información y asegurar el cumplimiento continuo de las normativas. Esto garantizará que los sistemas de protección sean resilientes ante ataques derivados de la computación cuántica.

Referencias

Bagozzi, R. y Phillips, L. (1982). *Representing and testing organizational theories: A holistic construal. Administrative Science Quarterly*, 27(1), 101-128.

OBSERVADOR DEL CONOCIMIENTO
Vol. 10 N° 5 (2025)
Edición Especial Ciencia y Tecnología Cuánticas | Tomo II

Barroso, M. (2016). *El Falsacionismo Popperiano: un intento inductivo de evadir la inducción.* EPISTEME vol. 36 Número1. Caracas jun. 2016. https://ve.scielo.org/scielo.php?script=sci_arttext&pid=S0798-43242016000100003

Bennett, C. y Brassard, G. (1984). *Quantum Cryptography: Public Key Distribution and Coin Tossing*. IEEE International Conference on Computers, Systems and Signal Processing.

Bernstein, D.; Buchmann, J. y Dahmen, E. (2009). *Post-Quantum Cryptography*. Springer.

Davenport, T. (1993). *Competing in Analytics. Harvard University. Hardvard Business Review*. https://cs.brown.edu/courses/cs295-11/competing.pdf

Floridi, L. (2012). *Semantic information and the network theory of account. Synthese*, 184 (3): 431-454, febrero 2012.

Floridi, L. (2010). *Information: A Very Short Introduction*. Oxford University Press.

Habermas, J. (1981). *The Theory of Communicative Action*. Beacon Press.

Ibrobo, S. (2020). *La teoría de la acción comunicativa de Jürgen Habermas. una interpretación y sus posibles aplicaciones en las ciencias de la gestión*. Revista Criterio Libre. https://revistas.unilibre.edu.co/index.php/criteriolibre/article/view/7538/6570#toc

Kant, I. (1785). *Groundwork of the Metaphysics of Morals*. Cambridge University Press.

Malishev, M (2014). *Kant: Ética del imperativo categórico.* La Comena 84 octubre-diciembre de 2014 pp. 9-21. ISSN 1405 6313.

Moore, G. (1996). *Crossing the chasm: Marketing and selling disruptive products to mainstream customers*. Harvard University. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496175

Nastidas, C. (2011). *La epistemología de la complejidad en el desarrollo crítico de la humanidad.* CDC v.28 n.77 Caracas. ISSN 1012-2508 https://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1012-25082011000200006

National Institute of Standards and Technology (NIST) (2023). *Post-Quantum Cryptography Standardization Process*.

Pirandola, S.; Laurenza, R.; Ottaviani, C. y Banchi, L. (2020). *Advances in Quantum Cryptography*. Nature Reviews Physics, 2(12), 711-726.

Popper, K. (1963). *Conjectures and Refutations: The Growth of Scientific Knowledge*. Routledge.

Porter, M. (1980). *Competitive Strategy: Techniques for Analyzing Industries and Competitors.* University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship, Available at SSRN: https://ssrn.com/abstract=1496175

Prigogine, I. (1997). *The End of Certainty: Time, Chaos, and the New Laws of Nature*. Free Press.

Shor, P. (1994). *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. IEEE Symposium on Foundations of Computer Science.

Veber, J. y Klima, T. (2014). *Influence of standards ISO 27000 family on digital evidence analysis. Paper presented at the IDIMT 2014: Networking Societies - Cooperation and Conflict, 22nd Interdisciplinary Information Management Talks, 103-111. Retrieved from* www.scopus.com.

Depósito legal: PP201402DC4456
ISSN: 2343-6212