

Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ciencias Matemáticas

Escuela Profesional de Computación Científica

Estudio del internet cuántico: implicancias y comparativa con el internet clásico

TESIS

Para optar el Título Profesional de Licenciado en Computación Científica

AUTOR

Yeeltsin Pool FERNANDEZ MENDOZA

ASESOR

Dra. Rosa Luz MEDINA AGUILAR

Lima, Perú

2024



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Fernandez, Y. (2024). *Estudio del internet cuántico: implicancias y comparativa con el internet clásico*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Escuela Profesional de Computación Científica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Yeeltsin Pool Fernandez Mendoza
Tipo de documento de identidad	DNI
Número de documento de identidad	47000609
URL de ORCID	No aplica
Datos de asesor	
Nombres y apellidos	Rosa Luz Medina Aguilar
Tipo de documento de identidad	DNI
Número de documento de identidad	10048247
URL de ORCID	https://orcid.org/0000-0002-0175-3894
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Edinson Raúl Montoro Alegre
Tipo de documento	DNI
Número de documento de identidad	09627181
Miembro del jurado 1	
Nombres y apellidos	Martha Hilda Timoteo Sánchez
Tipo de documento	DNI
Número de documento de identidad	09627181
Miembro del jurado 2	
Nombres y apellidos	Rosa Luz Medina Aguilar
Tipo de documento	DNI
Número de documento de identidad	10048247
Datos de investigación	
Línea de investigación	No aplica.
Grupo de investigación	No aplica

Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	Edificio: Facultad de Ciencias Matemáticas, Universidad Nacional Mayor de San Marcos. País: Perú Departamento: Lima Provincia: Lima Distrito: Cercado de Lima Av. Venezuela s/n cuadra 34. Lima 1-Perú Ciudad Universitaria. UNMSM. Latitud: -12.060186431587528 Longitud: -77.08213204783175
Año o rango de años en que se realizó la investigación	Abril 2024- octubre 2024
URL de disciplinas OCDE	Ciencias de la computación https://purl.org/pe-repo/ocde/ford#1.02.01 Ciencias de la información https://purl.org/pe-repo/ocde/ford#1.02.02

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
FACULTAD DE CIENCIAS MATEMÁTICAS
Escuela Profesional de Computación Científica

ACTA DE SUSTENTACIÓN DE TESIS PARA LA OBTENCIÓN DEL TÍTULO PROFESIONAL DE LICENCIADO EN COMPUTACION CIENTÍFICA (PROGRAMA DE TITULACIÓN PROFESIONAL 2024)

En la UNMSM – Ciudad Universitaria – Facultad de Ciencias Matemáticas, siendo las 20:15 horas del sábado 28 de setiembre del 2024, se reunieron los docentes designados como Miembros del Jurado Evaluador (PROGRAMA DE TITULACIÓN PROFESIONAL 2024): Dr. Edinson Raúl Montoro Alegre (presidente), Dra. Martha Hilda Timoteo Sánchez (miembro) y la Dra. Rosa Luz Medina Aguilar (miembro asesor), para la sustentación de la Tesis titulada: «ESTUDIO DEL INTERNET CUÁNTICO: IMPLICANCIAS Y COMPARATIVA CON EL INTERNET CLÁSICO» presentado por el Bachiller YEELTSIN POOL FERNANDEZ MENDOZA, para optar el Título Profesional de Licenciado en Computación Científica.

Luego de la exposición de la Tesis, el presidente invitó al expositor a dar respuesta a las preguntas formuladas.

Realizada la evaluación correspondiente por los Miembros del Jurado Evaluador, el expositor mereció la aprobación .....regular....., con un calificativo promedio de ..14 (catorce)..

A continuación, los miembros del Jurado Evaluador dan manifiesto que el participante Bachiller YEELTSIN POOL FERNANDEZ MENDOZA, en vista de haber aprobado la sustentación de su Tesis, será propuesto para que se le otorgue el Título Profesional de Licenciado en Computación Científica.

Siendo las 21:10 horas se levantó la sesión firmando para constancia la presente Acta.

Dr. Edinson Raúl Montoro Alegre
PRESIDENTE

Dra. Martha Hilda Timoteo Sánchez
MIEMBRO

Dra. Rosa Luz Medina Aguilar
MIEMBRO ASESOR

Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América

Vicerrectorado de Investigación y Posgrado

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

CERTIFICADO DE SIMILITUD

Yo, Rosa Luz Medina Aguilar en mi condición de asesor acreditado con la Resolución Decanal N.º 001300-2024-D-FCM/UNMSM de la tesis cuyo título es "*ESTUDIO DEL INTERNET CUÁNTICO: IMPLICANCIAS Y COMPARATIVA CON EL INTERNET CLÁSICO*", presentado por el bachiller YEELTSIN POOL FERNANDEZ MENDOZA para optar el título profesional de licenciado en Computación Científica. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 11% de similitud, nivel permitido para continuar con los tramites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título correspondiente.

Firma del asesor

DNI: 10048247

Nombres y apellidos del asesor: Rosa Luz Medina Aguilar



Dedicatoria

Dedico esta tesis a mis padres, Natividad y Lazaro, por su amor incondicional y apoyo constante. Su fe en mí y sus sacrificios me han motivado a alcanzar mis metas y a perseguir mis sueños.

A mi compañera de vida, Sharmely Madeleine Aguirre Rodas, por estar a mi lado en los momentos más difíciles y por ser mi mayor fuente de inspiración.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a todas las personas que han hecho posible la realización de esta tesis. En primer lugar, agradezco a mi asesora de tesis, la Dra. Rosa Luz Medina Aguilar, por su invaluable orientación, apoyo y paciencia a lo largo de este proceso. Sus comentarios y sugerencias han enriquecido enormemente mi trabajo y me han ayudado a crecer como investigador.

Agradezco también a mis profesores y compañeros de la Facultad de Ciencias Matemáticas por sus ideas y su compañerismo. Cada uno de ustedes ha contribuido a crear un ambiente de aprendizaje y motivación que ha hecho de mis años de estudio una experiencia memorable.

Yeeltsin Pool Fernandez Mendoza

Resumen

La presente tesis expone la implicancia del uso del internet cuántico en la transmisión de información. Para ello se procederá a describir los conceptos fundamentales de internet cuántico y los aspectos más importantes sobre su uso en la transmisión de información. Además, esta tesis utilizará una metodología descriptiva con el objetivo de realizar un estudio a nivel histórico donde resaltaremos los hitos principales en el desarrollo del internet clásico y el internet cuántico el cual es una tecnología que utiliza principios o conceptos basados en teoría cuántica como el entrelazamiento y la superposición, los cuales son fundamentales para transmitir y analizar datos de manera más segura y eficiente que el ya conocido internet tradicional, demostrando que esta tecnología transformaría la capacidad de recopilación de datos, la seguridad, la integridad de las transmisiones y la confiabilidad de los resultados mediante a través del qubit. Aunque al ser una tecnología experimental también posee algunas limitantes como la decoherencia y la fragilidad de los qubits que podrían afectar la eficiencia antes mencionada. Asimismo, la presente tesis presenta un estudio comparativo entre el internet cuántico y el internet clásico para finalmente mostrar las implicancias que tendría en "seguridad de la información" del usuario y en "transmisión de datos". Cabe resaltar que, debido a la falta de acceso a las instituciones donde tienen lugar las investigaciones para llevar a cabo las pruebas planificadas para este propósito, es crucial destacar que esta tesis se basará en las aprendizajes y evidencias publicadas por los investigadores del tema.

Palabras claves: Computación cuántica, teoría cuántica, internet cuántico, internet clásico, transmisión, procesamiento, seguridad.

Abstract

This thesis entitled “Study of the quantum internet: Implications and comparison of the classical internet” has the objective of exposing the implication of the use of the quantum internet in the transmission of information. For them, the fundamental concepts of the quantum internet and the most important aspects of its use in the transmission of information will be described. Furthermore, this thesis will use a research methodology with the objective of carrying out a historical study highlighting the main milestones in the development of the classical internet and the quantum internet, which is a technology that uses notions of quantum theory to transmit and process data from a safer and more efficient way than the already known traditional Internet, demonstrating that this technology would transform the data collection capacity, the size of data exchanged and the reliability of the results thanks to the qubit as a quantum programming unit. Likewise, this thesis presents a comparative study between the quantum internet and the classical internet to finally show the implications it would have on the security of user information and data transmission. It should be noted that, due to the lack of access to the institutions where the research takes place to carry out the tests planned for this purpose, it is crucial to highlight that this thesis will be based on the learning and evidence published by researchers on the topic.

Keywords: Quantum computing, quantum theory, quantum internet, classical internet, transmission, processing, security.

Índice de Contenido

INDICE DE FIGURAS 8
INDICE DE TABLAS 9
INTRODUCCIÓN 10
CAPITULO 1 12
ASPECTOS GENERALES DE LA TESIS 12
1.1. Definición del Problema 12
1.1.1. Descripción del Problema 12
1.1.2. Formulación del Problema 13
1.2. Definición de objetivos 13
1.2.1. Objetivo general 13
1.2.2. Objetivos específicos 14
1.3. Alcances y limitaciones 14
1.3.1. Alcances 14
1.3.2. Limitaciones 14
1.4. Justificación 14
1.5. Estado del Arte 15
CAPITULO 2 18
MARCO TEÓRICO 18
2.1. Fundamento teórico 18
2.2. Marco conceptual 23
CAPITULO 3 30
EL INTERNET CUÁNTICO COMO NUEVA ALTERNATIVA 30
3.1. Desarrollo histórico del internet clásico 30
3.2. El internet clásico en la actualidad 33
3.3. Desarrollo Histórico del Internet cuántico 37
3.4. El internet cuántico en la actualidad 40
3.4.1. Arquitectura de una computadora cuántica 42
3.4.2. El internet cuántico y sus Casos de éxito hasta la actualidad 44
3.5. Similitudes y diferencias entre el Internet clásico e Internet cuántico 48
3.6. Implicancias en la seguridad 49
3.6.1. El internet clásico en protección de la información 49
3.6.2. El internet cuántico y sus implicancias en la seguridad de la información 56
3.7. Implicancias en la transmisión de la información 58
CONCLUSIONES 60
Bibliografía 61

INDICE DE FIGURAS

Figura 1 Estado de un qubit. 20
Figura 2 Problema de comunicación 26
Figura 3 Criptografía Clase privada 27
Figura 4 Criptografía Clave pública 28
Figura 5 IP Clase A 34
Figura 6 Protocolos TCP/IP 35
Figura 7 Los transmisores, receptores y rendimiento del APT 46

INDICE DE TABLAS

Tabla 1 Resumen de la conversión de petabytes en todas las unidades comunes 36
Tabla 2 Comparativo de Internet clásico e Internet cuántico 48
Tabla 3 Tipos de Cifrado simétrico 50
Tabla 4 Comparación de claves ECC y RSA 50

INTRODUCCIÓN

En la actualidad, sabemos sobre el uso del internet al cual llamaremos internet clásico forma parte del día a día de todas las personas que usan equipos electrónicos y cuenta con sistemas de automatización que interactúan con el ser humano con el propósito de mejorar el estilo de vida y hacer más fácil el día a día, lo cual lo hace de uso masivo a nivel mundial, asimismo se enfrenta a problemas cada vez mayores en términos de seguridad, privacidad, transmisión de información y otros. Además, con la creciente amenaza de ciberataques y filtraciones de datos, apremia la creación de una red de comunicación más segura, esto ha llevado a la ciencia a querer buscar alternativas innovadoras para tratar de resolver la mayoría de los problemas que actualmente enfrenta el internet clásico.

Es ahí donde se da paso el internet cuántico, el cual podemos decir que es un concepto emergente que usa las nociones principales de la mecánica cuántica y de la teoría de la información cuántica, el cual promete revolucionar nuestras comunicaciones digitales al superar las limitaciones del internet clásico y ofrecer mejoras en seguridad, eficiencia y velocidad. Aunque todavía queda un largo camino por delante para poder utilizar sus aplicaciones prácticas definitivas, el internet cuántico es la siguiente gran revolución tecnológica, muestra de ello son los primeros logros empiezan a darse en investigaciones llevadas a cabo a nivel mundial, con lo cual se está preparando el terreno para una transformación total del internet como lo conocemos.

Por ello, esta tesis plantea exponer la implicancia del uso del internet cuántico en la transmisión de información, su desarrollo histórico, similitudes con el internet clásico asi como sus implicancias en un tema importante como es la seguridad de la información.

Con el fin de conseguir el objetivo de la tesis, en su conjunto se ha dividido en cuatro capítulos de la siguiente manera:

En el primer capítulo se desarrollan la situación problemática, la formulación del problema, los objetivos del proyecto, el alcance y limitaciones de esta tesis.

El segundo capítulo proporcionará el marco teórico y abordará conceptos relacionados con el estudio del internet cuántico, tales como la física cuántica, la máquina de Turing, el internet, el ordenador cuántico y culminará con la computación cuántica en la criptografía.

En el tercer capítulo señalaremos ampliamente el desarrollo histórico tanto del internet clásico como el internet cuántico y señalaremos cómo este último es una novedosa alternativa para una mejor transmisión de datos. Asimismo, expondremos las similitudes y diferencias para culminar con las implicancias en la seguridad y transmisión de información donde se explicarán los transcendentales descubrimientos de los estudios y casos de éxitos realizados en el mundo sobre esta temática y como estos resultados sustentan el uso del internet cuántico como herramienta para mejorar la seguridad de transmisión de información en la red. Finalmente, las conclusiones que se llegaron al analizar la información estudiada se presentarán en el cuarto capítulo.

CAPITULO 1

ASPECTOS GENERALES DE LA TESIS

1.1. Definición del Problema

1.1.1. Descripción del Problema

Existen tres pilares de seguridad que toda información debe cumplir con: confidencialidad, integridad y autenticidad. En términos de confidencialidad significa a la protección de la información sensible para que no sea divulgada a personas o sistemas que no están autorizados. La integridad garantiza que la información sea preciso y completo, y la disponibilidad de la información garantiza que esté disponible cuando se necesite (Fuentes Herrera, 2017).

Debido a esto, y convirtiendo a toda información en un bien valioso, las organizaciones han creado tareas particulares de seguridad en la tecnología de la información o también conocido como TI por sus siglas, incluido el uso de técnicas y herramientas que garanticen la preservación de los fundamentos de la información.

La seguridad de las actividades y transacciones realizadas en Internet se define como seguridad en Internet. Es una parte específica de los conceptos fundamentales de seguridad informática y ciberseguridad; incluye asuntos como la seguridad de las redes, el comportamiento en línea y la seguridad de los navegadores. Se incluyen entre los importantes peligros a la seguridad en Internet las siguientes:

- Hackeo, es decir cuando personas no autorizadas acceden a sistemas, cuentas de correo electrónico o sitios web.
- El *malware*, que es un virus o software malicioso que puede perjudicar los datos o exponer los sistemas a otras amenazas.
- *Phishing* o sustracción de identidad del usuario, que permite a ciberdelincuentes sustraer información financiera y personal que tiene en los servicios tecnológicos como aplicativos.

Los sistemas de protección que surgen como resultado de la necesidad de resguardar la información e incluyen algoritmos matemáticos y funciones que otorgan permisos para cifrar y cuidar la información, garantizando la seguridad de las transferencias de datos.

Como alternativa, el internet cuántico es una opción para perfeccionar la seguridad de la transmisión de datos, ya que el bit cuántico es la unidad de almacenamiento principal y cada uno pueden tener varios estados al mismo tiempo en un instante determinado. (Ramírez *et al*., 2021), y asi la vulnerabilidad de la transmisión de información disminuye radicalmente.

1.1.2. Formulación del Problema

Uno de los principios más básicos de la mecánica cuántica es el principio de incertidumbre de Heisenberg, el cual establece que es imposible conocer simultáneamente la posición y el momento (o velocidad) de una partícula con precisión arbitraria. Cuanto más precisamente tratemos de medir una de estas magnitudes, menos precisión tendremos en la medida de la otra. Esta limitación no se debe a fallos en los instrumentos de medición, sino que es una propiedad fundamental de la naturaleza cuántica. Esto implica que las partículas no pueden ser descritas en términos de valores exactos de posición y momento, sino más bien en términos de probabilidades. Por tal motivo, la capacidad de las partículas cuánticas de existir en estados indefinidos se ha utilizado para mejorar el cifrado de datos, esto está relacionado al campo de la criptografía cuántica, que aprovecha las propiedades cuánticas, como la superposición y el entrelazamiento, para asegurar la transmisión de datos. Es por ello por lo que algunos investigadores argumentan que podrían usar la mecánica cuántica para lograr mejoras, aprovechando la extraña capacidad de la naturaleza para entrelazar objetos distantes y teletransportar información entre ellos. Es por ello por lo que el problema que se proyecta en esta tesis es **¿Qué implicaciones tendría el internet cuántico en la transmisión de información?**, es decir en qué aspectos mejorará la seguridad en las computadoras, cómo podremos resguardar ante este nuevo descubrimiento y si estamos preparados para este cambio, en otras palabras, cuántos cambios podremos implementar en nuestra información real.

1.2. Definición de objetivos

1.2.1. Objetivo general

Exponer las implicancias de la utilización de internet cuántico en la transmisión de información.

1.2.2. Objetivos específicos

- Describir en términos generales el internet cuántico y los aspectos más significativos de su uso en la transmisión de información.
- Exponer la relación entre el uso del internet cuántico y la mejor transmisión de datos.
- Documentar los aportes más importantes del internet cuántico y los componentes que lo componen.
- Analizar la evolución desde el principio del internet cuántico y sus principales aspectos.

1.3. Alcances y limitaciones

1.3.1. Alcances

La presente tesis es un estudio descriptivo sobre la transmisión de la información y lo que pretende es estudiar las alcances que posee el internet cuántico y sus implicancias en la transmisión de información, apoyada en las divulgaciones acerca de la física cuántica.

1.3.2. Limitaciones

La presente tesis se apoyará en las experiencias y resultados publicados hasta la actualidad, ya que al no contar con acceso a los centros de investigación no se podrán realizar las pruebas diseñadas en dichos estudios, por esta limitante no se incluirán.

1.4. Justificación

Cabe destacar que, en el desarrollo de la informática, el conocimiento ha evolucionado y se ha transformado en una parte crucial de las organizaciones, porque actualmente estamos buscando transacciones rápidas con el uso de la red, por ello que aplicaciones, modernas tecnologías y los programas de información han cambiado la forma en que las empresas operan. Asimismo, la seguridad se ha transformado en crucial y los equipamientos deben ser seguros, asegurables y accesibles en cualquier situación para proteger la información. Con esta tesis se quiere generar un precedente sobre el uso del internet cuántico y sus implicancias en la transmisión de información. Ya que el uso de Internet cuántico podría permitir la transmisión de información en trayectorias extensas y a frecuencias aún mayores a las actuales.

1.5. Estado del Arte

La aplicación de la tecnología cuántica no es tan nueva como se cree, ya que algunas organizaciones como D-Wave Systems, fundada en 1999, y que desarrolló prototipos de computadoras cuánticas y haber vendido la primera computadora cuántica comercial en 2011. Aunque esto fue solo el comienzo, es muy probable que representen un hito en la informática y la computación en general; es por ello que muchos investigadores la consideran una revolución informática.

El internet cuántico emplearía fotones de luz para la transmisión de datos; además, sustituiría al bit tradicional con una unidad de datos nueva llamada qubit. “El cúbit, que sustituye al bit, puede ser al mismo tiempo 0 y 1, debido a las leyes de la mecánica cuántica aplicada a los átomos”. Al utilizar las propiedades de la física cuántica, como el entrelazamiento de partículas el internet cuántico es más seguro contra hackeos. Esto significa que cualquier intento de interceptar los datos altera el estado de las partículas, lo que alerta a los usuarios sobre la presencia de un intruso. Además, esto permite canales de comunicación inherentemente seguros, protegiendo la información durante su transmisión. Esto implica que la red cuántica sería más segura y que su tecnología es mucho más rápida debido a sus características (Luna, 2003, p. 19).

La creación de una red segura para la transmisión de datos mediante el internet cuántico es uno de los hallazgos más significativos de estudio realizados entre investigadores interesados sobre este tema como por ejemplo el. Otros resultados incluyen la conexión a grandes redes terrestres, como por ejemplo primero en Europa y China, y conexiones multiparte desde satélites a varias estaciones terrestres en paralelo (Claramunt Carriles, 2022).

En ese sentido, y tal como lo señala López, China cuenta con una gran cantidad de recursos enfocados en el desarrollo de las comunicaciones cuánticas y estos últimos años ha logrado enviar con gran éxito un mensaje cifrado que no se puede violar entre dos estaciones terrestres.

La implantación de redes cuánticas sobre redes comerciales de fibra óptica lleva acompañada la necesidad de la gestión de estas. En un escenario de explotación comercial, surgen las necesidades de disponibilidad de la red, garantía de calidad de servicio y capacidad de recuperación frente a incidencias sobrevenidas.

La distribución de repetidores cuánticos para crear redes cuánticas comerciales es uno de los métodos utilizados en los principales estudios de investigación (Iván García-Cobo, 2022).

Asimismo, en la actualidad, se han descubierto técnicas y cálculos matemáticos con objeto de lograr el cifrado, el descifrado y las claves en la criptografía de internet cuántico. La criptografía asimétrica utiliza la clave pública y la clave privada del receptor del destinatario para cifrar y descifrar, mientras que la criptografía simétrica es un tipo de algoritmo que utiliza una misma clave para cifrar y descifrar, y el hash algoritmo, que transforma un bloque de datos en una nueva serie de caracteres de longitud fija, independientemente del bloque de datos de entrada, y el destinatario tiene su clave privada y pública (Claramunt Carriles, 2022).

En relación con los hallazgos de las diversas investigaciones y estudios sobre el internet cuántico, tenemos un estudio realizado en China donde los científicos de la Universidad de Ciencia y Tecnología de China han realizado investigaciones creando Zuchongzhi, un supercomputador cuántico con una capacidad de 66 cúbits (Qubits meet materials science, 2021). Conforme sus creadores, es competente para completar una actividad de gran complejidad, que en los supercomputadores más potentes actuales requeriría al menos 8 años, en aproximadamente 1,2 horas (Wu *et al*., 2021). La empresa multinacional de corte tecnológico International Business Machines Corporation o más conocida por sus siglas IBM, también presenta su procesador cuántico de 127 cúbits llamado Eagle. La capacidad de Zuchongzhi, que hasta ahora era la más avanzada, se ha duplicado con Eagle. Este procesador ha superado con creces lo que se podía simular con procesadores clásicos. También, en 2022, investigadores como Noiri, A., Takeda, K., Nakajima, T. *et al*. (2022) han logrado obtener una precisión superior al 99%, lo que significa que los errores que el ordenador cuántico comete no son comunes. Asimismo, estos experimentos se llevaron a cabo con uno o dos cúbits, por lo que se requeriría descubrir cómo extender esta tecnología a computadoras con muchos más cúbits. Por lo que investigadores como Noiri (2022) afirman que los protocolos cuánticos de corrección de errores funcionan bien con errores menores al 1%.

Según la tendencia de las investigaciones realizadas sobre el tema, el internet cuántico es una fuente muy poderosa que será accesible en un futuro cercano . Esta nos brinda numerosas ventajas en términos de protección y, especialmente, en términos de

velocidad de procesamiento (Liu *et al*., 2024; Wu *et al*., 2021), lo cual es un problema importante en la actualidad con la red tradicional pero que podemos solucionar fácilmente con la red cuántica.

CAPITULO 2

MARCO TEÓRICO

2.1. Fundamento teórico

Tal como se expuso en el capítulo pasado, el internet cuántico cuenta con características como el entrelazamiento cuántico y la teleportación cuántica, las leyes, la tecnología cuántica y las herramientas que regulan estas áreas facilitan la creación de una red de comunicaciones ultra segura de utilizar para un futuro. Es por ello que la presente tesis se fundamentará en teorías y conceptos como la física cuántica, el método de distribución de claves cuánticas, la máquina cuántica de Turing entre otros, los cuales serán desarrollados a continuación.

La **física cuántica** según R. Shankar (1994), es una teoría fundamental que describe la naturaleza del mundo en escalas muy pequeñas, como las de los átomos y las partículas subatómicas. Esta tería tiene los siguientes aspectos clave:

- Principio de incertidumbre: La física cuántica desafía la intuición clásica, especialmente a través del principio de incertidumbre de Heisenberg, que establece que existe un límite fundamental en la precisión con la que se pueden conocer simultáneamente ciertas propiedades de un sistema, como la posición y el momento.
- Dualidad onda-partícula: Shankar enfatiza que los objetos cuánticos, como electrones y fotones, no se comportan exclusivamente como partículas o ondas, sino que exhiben características de ambos dependiendo de la situación y cómo se mida el sistema.
- Superposición: En la interpretación cuántica, un sistema puede existir en múltiples estados a la vez (superposición) hasta que una medición colapse ese estado en uno específico. Esto implica que la realidad cuántica es inherentemente probabilística y no determinista.
- Función de onda: La función de onda, que describe el estado cuántico de un sistema, contiene toda la información sobre el sistema y es fundamental en la formulación de la mecánica cuántica. Shankar explica su papel en las predicciones probabilísticas y cómo se relaciona con los observables a través de los operadores.
- Matematización: Shankar utiliza un enfoque matemático riguroso, pero accesible, para desarrollar de forma lógica y coherente los conceptos cuánticos, mostrando cómo estos principios llevan a resultados cuantificables y a predicciones verificables experimentalmente.

- Relación con la realidad física: Shankar discute cómo la mecánica cuántica se relaciona con la realidad física y cómo ha sido confirmada a través de numerosos experimentos, destacando su poder para explicar fenómenos que no pueden ser abordados desde la física clásica.

Por lo tanto, la física cuántica es un marco teórico esencial que redefine nuestra comprensión de la naturaleza en niveles fundamentales, utilizando matemáticas para formalizar conceptos que van más allá de la lógica clásica. Su tratamiento de la materia busca conectar la teoría con la observación experimental, subrayando la importancia de la naturaleza probabilística y la complejidad inherente del mundo cuántico (Shankar, 1994).

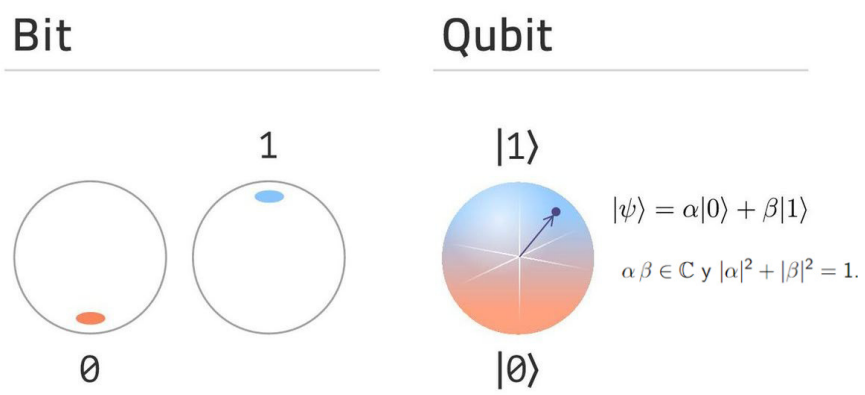
ha llegado a revolucionar la tecnología, algunas de sus soluciones incluyen la fibra óptica, la inteligencia artificial y las comunicaciones. La seguridad informática podría verse significativamente alterada por la física cuántica, en particular. Será imposible hackear la transmisión sin dejar rastro, lo cual es la principal virtud de esta tecnología. Cabe resaltar que un ordenador tradicional se basa en código binario de operaciones con bits para almacenar y procesar información en un lenguaje de ceros y unos. La base de la informática clásica es la lógica de que un elemento solo puede ser una cosa a la vez, o un "0" o un "1". En la información cuántica, estos ceros y unos se superponen simultáneamente.

Cabe resaltar que el principio de superposición se emplea en los sistemas cuánticos, lo cual explica la conocida paradoja del gato de Schrödinger, el cual nos dice que cuando se coloca una caja con un gato dentro cerrada junto con un aparato que contiene sustancia radioactiva, un contador Geiger y un veneno, el dispositivo está diseñado de tal manera que, si el contador Geiger detecta radiación, se rompe un frasco de veneno y el gato muere; si no se detecta radiación, el gato vive. Este experimento es una forma de ilustrar cómo los principios de la mecánica cuántica pueden parecer contradictorios o contraintuitivos en comparación con nuestra experiencia diaria del mundo. Así, un qubit puede tener un estado donde el valor puede ser 1 y 0 a la vez:

$$|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle \qquad (1)$$

Donde $c_0, c_1 \in \mathbb{C}\ |c_0|^2 + |\,c_1|^2 = 1$.

Figura 1 Estado de un qubit.



Fuente: Adaptado de Hutterstock, 2018.

Por esta razón y tal como se muestra en la figura 1 podemos explicar que un bit, el cual es la unidad mínima en el internet clásico, representa a un sistema con dos estados. Se puede distinguir en una de estas áreas, los cuales representa dos valores matemáticos como 1 ó 0, sí ó no, verdadero ó falso y así (Pastor Collado & Elias Vila, 2017). La ventaja tanto del internet cuántico con respecto a la información cuántica sobre sus contrapartes clásicas no es que un qubit no tenga un valor determinado, sino que radica en el paralelismo y el entrelazamiento cuánticos.

Es asi que, asegurar comunicaciones seguras de extremo a extremo es el objetivo de la criptografía cuántica, que crea claves seguras a partir de las leyes fundamentales de la mecánica cuántica. Con fin de proteger la información de los ataques, se han creado parámetros de seguridad particulares

Desde ese punto de vista, en algún momento, se espera que estas organizaciones más seguras sustituyan a los sistemas de comunicación que ya existen.

Un experimento importante en relación con el internet cuántico sobre la comunicación cuántica, el cual da cuenta del entrelazamiento cuántico que usa satélites. Un ejemplo notable es el satélite Micius (también conocido como QUESS, Quantum Experiments at Space Scale), lanzado por China en 2016.

Este satélite ha llevado a cabo experimentos de entrelazamiento cuántico a largos distancias, permitiendo la transmisión de información cuántica segura. En estos experimentos, se ha logrado la transmisión de fotones entre dos estaciones en la Tierra separadas por más de 20,000 km, lo que demuestra la posibilidad de realizar

comunicaciones cuánticas sin que la información se pierda, gracias a la naturaleza del entrelazamiento cuántico (Liao, S.-K., *et al*, 2017).

En igual forma, otro fundamento teórico importante son las comunicaciones a través del **método de distribución de claves cuánticas,** el autor Sharma (2021) nos menciona que es conocido como QKD, por su traducción al inglés de "distribución de claves cuánticas", que se refiere a una técnica para cifrar datos utilizando las características de la mecánica cuántica. Asimismo, el QKD incluye bits cuánticos, sistema QKD básico, Esquemas QKD y familias de protocolos junto con la descripción detallada del proceso QKD basado en el protocolo Bennett y Brassard-84 (BB84), ya que es el protocolo QKD más utilizado en la literatura. (Sharma, 2021).

Asi como el protocolo E91 criptográfico fue desarrollado por Artur Ekert en 1991 y se encuentra basado en el Teorema de Bell (Bell, 1964). El protocolo E91 utiliza fotones entrelazados. Estos pueden ser preparados por Alice, Bob o algún tercero, y son distribuidos de manera que Alice y Bob tengan un fotón de cada par. El modelo se fundamenta en propiedades del entrelazamiento cuántico.

Esta tecnología QKD hace que sea imposible interceptar las comunicaciones porque detecta rápidamente cualquier interferencia. De este modo, cualquier intento de pirateo de dicha señal supondría la autodestrucción inmediata de la comunicación evitando así la pérdida de información. La posibilidad de conexión entre distancias significativas ha sido el mayor problema que han hecho frente los investigadores. Según Sharma, el éxito principal del experimento se debe al uso de catadióptricos pasivos que se refieren a componentes ópticos que utilizan principios de reflexión y refracción para manipular fotones sin la intervención activa de fuentes de energía externas, como láseres o dispositivos electrónicos, los cuales están establecidos en satélites para conservar completamente las señales luminosas de extensa distancia. Por lo tanto, los avances evidenciados en este estudio más reciente nos conducen a creer que en un futuro cercano será una red de internet altamente segura debido al uso de la criptografía cuántica.

Tanto como el desarrollo y aplicación de esta crearía un nuevo espacio de comunicación que favorecería de manera directa las acciones a nivel comercial. Los consumidores aumentarían su confiabilidad en la transmisión de datos ya sean personales o no, a través de las redes, a la vez que las instituciones podrían tener acceso a cualquier plataforma online sin preocupación al tráfico de información.

La creciente frecuencia de ciberataques y el desarrollo del internet cuántico plantean desafíos para salvaguardar la infraestructura actual de tecnologías de la información de los usuarios los cuales hay una interacción entre ellos.

"La distribución de claves cuánticas (QKD) ha sido objeto de muchas investigaciones en los últimos años y se considera una tecnología prometedora para crear redes seguras. Las redes troncales terrestres, submarinas, metropolitanas y de acceso utilizan fibra óptica para transportar una gran cantidad de información. Por lo tanto, la integración de QKD con las redes ópticas clásicas existentes se ha propuesto como una solución rentable en lugar de usar fibras oscuras separadas para la comunicación cuántica. Sin embargo, esta integración presenta nuevos desafíos de investigación"(Sharma, 2021).

Otro fundamento para el internet cuántico es la máquina cuántica de Turing y a pesar de que Feynman fue el pionero en sugerir que los ordenadores cuánticos tendrían mayores ventajas que los clásicos en simular sistemas físicos. Sin embargo, el cambio de paradigma computacional se debió principalmente a los desafíos que enfrentó la tesis de Church-Turing con el surgimiento de la teoría de la complejidad en los setenta. La teoría se enfoca en la cantidad de recursos que requiere un computador para realizar un algoritmo específico, especialmente en términos de tiempo de cálculo y memoria de almacenamiento. Además de la equivalencia entre los algoritmos y las máquinas de Turing, se requería que los algoritmos fueran eficientes, es decir, que pudieran ser incluidos en la clase P de problemas resolubles en tiempo polinómico en relación al tamaño de su cadena de entrada o, que se puede definir como problemas resolubles en tiempo polinómico con una ayuda, ejemplo o testigo de tamaño polinómico, como la comprobación de primalidad de un número (Ruiz, 2021).

Son problemas cuyas soluciones positivas se pueden verificar en tiempo polinómico. También existe la clase complementaria, coNP, de problemas cuyas respuestas negativas también se pueden verificar en tiempo polinómico. Por lo tanto, las máquinas deterministas clásicas de Turing parecían no cumplir con la tesis de Church-Turing, que requería eficiencia adicional. Esto contrastaba con otros algoritmos de tipo probabilístico que se descubrieron en el contexto de la primalidad mencionado (Solovay y Strassen 1977). Por admitir subrutinas simultáneas, los algoritmos de la clase NP están relacionados con el mundo no determinista (y cuántico). Aunque es evidente que $P \subseteq NP$, el problema de que estas dos clases coincidan sigue siendo un problema abierto. Los especialistas en informática como Aaronson (2013) sostienen que $P \subseteq NP$, ya que negarlo equivaldría a

afirmar que la creatividad en matemáticas se puede automatizar, al mismo tiempo que la capacidad de verificar una prueba implica la capacidad de encontrar una (Aaronson, 2013). El problema P = NP fue nombrado el tercero de los siete problemas del milenio definidos en 2000 por el Clay Mathematics Institute y galardonado con un millón de dólares. Esto se debe a que conocer el método para verificar que una solución positiva de un problema es cierta equivale a resolver el problema, independientemente de su complejidad.

Por lo tanto, Deutsch extendió la tesis afirmando que un modelo universal de computadora trabajando con medios limitados podría simular perfectamente cada sistema físico para tener en cuenta estas complejidades basado en las teorías de Church-Turing. (Deutsch 1985, p. 99). Las máquinas de Turing no pudieron aceptar este principio en la física clásica porque los estados de la dinámica clásica eran continuos. Y basándose en la prueba del carácter mecánico cuántico de la naturaleza, descubrió que ese principio más general podría ser alcanzado en el contexto de la mecánica cuántica, siguiendo un razonamiento similar al de Feynman. A pesar de su ilustración del modelo computacional universal cuántico, que demostraba la eficacia del cálculo cuántico en comparación con el cálculo clásico, la prueba de su suposición con altas expectativas en la que se reconoce que la computación cuántica realiza varias tareas mejor que la computación clásica. La aceleración cuántica (speedup) ya es algo aceptado en toda la comunidad científica. Sin embargo, los autores como Lov Grover y Peter Shor (Shor 1994; Grover 1996), que encontraron pruebas en los noventa a favor de la eficiencia de la computación cuántica, abrieron el camino experimental para los esfuerzos de Turing para materializar las máquinas o computadoras cuánticas.

2.2.Marco conceptual

Internet es la red global de redes de computadoras que permiten la comunicación y el intercambio de datos. Es una gran red de computadoras, cada uno de ellos es autónomo e independiente. Internet ha experimentado una rápida evolución desde su fundación y actualmente incluye una variedad de servicios, siendo el más conocido el World Wide Web. La web está hecha de millas para computadoras interconectadas donde se puede transferir cualquier tipo de información multimedia, como texto, imágenes, video, sonido, etc.

La **fibra óptica** es el medio de transmisión preferido: en la actualidad, los cables que se han extendido por los océanos, el aire y la tierra conectan continentes y regiones separadas en la comunidad global que hoy tenemos. Esto ha llevado al desarrollo de nuevos dispositivos relacionados con esta tecnología, como circuladores ópticos, amplificadores, compensadores, multiplexores, demultiplexores, WDM, aisladores, controladores de polarización, fuentes de luz, etc. (Schott, 2022)**.**

Los **sistemas de fibra óptica** utilizan la transmisión de luz a través de fibras de vidrio o plástico para enviar datos y tienen una serie de ventajas significativas sobre otros utilizados en la transmisión y el tratamiento de señales analógicos y digitales (Aristizabal, 2017).

El **internet cuántico**, se conceptualiza como una red basada en principios cuánticos que permite la transmisión y procesamiento de información utilizando partículas cuánticas, como fotones, de manera que aproveche las propiedades únicas de la mecánica cuántica. Cabe resaltar que existe una de una infraestructura que permita la interconexión de nodos cuánticos, donde cada nodo puede realizar operaciones cuánticas y almacenar estados cuánticos. Esta infraestructura es esencial para facilitar la comunicación cuántica a larga distancia (Fang *et al*., 2023).

Asimismo, debemos destacar la importancia del entrelazamiento cuántico, que permite la correlación instantánea entre partículas separadas por grandes distancias. Esto es fundamental para protocolos como la teleportación cuántica y la distribución de claves cuánticas. Por otro lado, el intenet cuántico implica protocolos de Comunicación que permiten la transferencia de información cuántica, como la teleportación cuántica y la criptografía cuántica, que aseguran que la información no sólo sea transmitida de manera eficiente, sino también de forma segura. No obstante, y tal como lo menciona Fang *et al*., (2023) el internet cuántico puede superar algunas limitaciones del internet clásico, ofreciendo potencialmente comunicaciones más seguras y eficientes gracias a las propiedades cuánticas de la información, pero la implementación del internet cuántico también enfrenta desafíos, como la fidelidad de la transmisión, la corrección de errores y la necesidad de nuevas tecnologías de detección y manipulación de estados cuánticos.

Un **ordenador cuántico** lograría completar una amplia gama de tareas de manera significativamente más rápida que las mejores supercomputadoras del mundo presentes y futuras. Sin embargo, antes o después, los computadores cuánticos deberán establecerse en una red que no altere la naturaleza cuántica de la información que circula por ella, dejando

de lado su poder computacional. Eugene Polzik, mencionó en un artículo publicado en la **revista Nature, desarrolló un dispositivo que podría ser el primer paso hacia una futura red** de computación cuántica (Sillanpää & HakonenPertti J. Hakonen, 2015).

- **Medidas cuánticas**: En este caso, un **estado** cuántico conocido como qubit sirve como representación física de los átomos. En contraste con el bit tradicional, este bit no es binario:

  $$|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle. \quad (2)$$

  La siguiente es su expresión formal. Para representar estados cuánticos, se utiliza la notación de Dirac, que se acompaña de las bases $|0\rangle$, $|1\rangle$. La condición es ortonormal. Entonces, c_0, c_1 siguen la relación $|c_0|^2 + |c_1|^2 = 1$ siendo c_0, $c_1 \in \mathbb{C}$. La toma de medidas sobre la ecuación 1 es irreversible y el resultado es una medida 0 o 1 de un bit convencional. En la toma de medidas, hay muchos ejemplos: si $|\psi\rangle = |0\rangle$, o $|\psi\rangle = |1\rangle$, cualquier medida colapsará a 0 o 1. Sin embargo, al medir el fotón, el resultado ser 0, pero no ambos. Estos resultados se corresponden con las probabilidades $|c_0|^2$ y $|c_1|^2$, respectivamente.

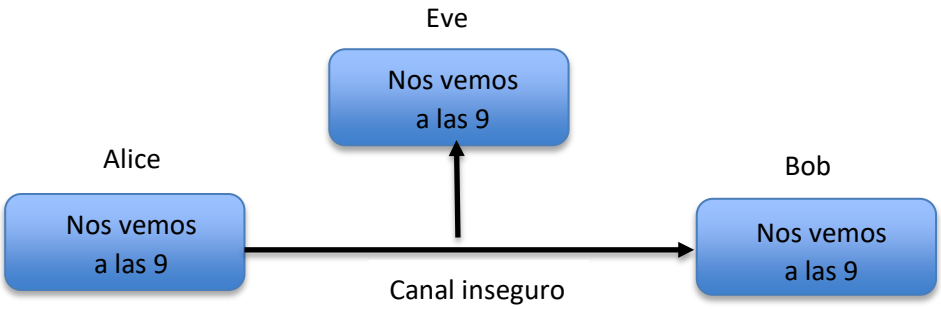
  Una interacción directa con un estado cuántico supone una operación de medida. Este concepto es crucial para entender a los canales cuánticos en las comunicaciones: en protocolos haciendo uso de ambos tipos de canal, en el clásico, puede compartirse información que no es crítica en cuanto a seguridad. Mientras tanto, al ser el espionaje sobre un canal cuántico completamente detectable gracias a la alteración del estado cuántico en sus envíos, es razonable que se utilice para transmitir la información de clave. Si se intenta atacar al canal, en el protocolo encontrarán unas tasas de acierto erróneas entre el emisor y el receptor que, de detectarse, se abortará el protocolo (Aguado, 2022).
- Qubits: se puede existir en una superposición de ambos estados simultáneamente. Esto significa que un qubit puede representar 0, 1, o cualquier combinación de ambos al mismo tiempo, gracias a las propiedades de la mecánica cuántica. Los qubits deben tener dos características cruciales: superposición y entrelazado cuántico. La superposición es uno de los principios fundamentales de la mecánica cuántica que permite que los qubits tengan un comportamiento muy diferente al de los bits clásicos. En un sistema de computación cuántica, la superposición significa que un qubit puede estar en múltiples estados al mismo tiempo. El entrelazado cuántico se refiere a la

propiedad cuántica en la que un sistema de dos niveles (en este caso un qubit) se encuentran en un estado conjunto tal que las propiedades de uno de ellos están intrínsecamente relacionadas con las propiedades del otro, sin importar la distancia que los separa. Esta propiedad desafía nuestras intuiciones clásicas sobre la separación y la independencia de los objetos. De esta manera, se pueden formar grupos de qubits simultáneamente y manipularlos como si fueran uno. La razón de la "aceleración" cuántica (speedup) se debe al paralelismo cuántico.

- **La computación cuántica en la criptografía:** La criptografía cuántica es una técnica de la criptografía que utiliza la física cuántica para enviar datos de forma que solo el destinatario previsto consiga acceder a ella.

  Para alcanzar una explicación detallada de la criptografía cuántica, es necesario adquirir algunos conceptos básicos de criptografía y física cuántica. Estos conceptos ayudarán a comprender mejor el fondo. Sin embargo, antes que nada se presenta el problema que la criptografía cuántica intentará resolver.

Figura 2 Problema de comunicación



Fuente: Elaboración propia.

Dos personajes principales, Alice y Bob, están involucrados en un problema que se presenta en la figura número 2. Alice tiene la intención de comunicarse con Bob, pero como no están en el mismo lugar, lo hará mediante un enlace. El tercer personaje, a quien llamaremos Eve, introduce el problema en cuestión. Eve intentará escuchar la conversación entre Alice y Bob, pero al mismo tiempo no desean ser escuchados.

Numerosos enfoques se utilizan en la criptografía para evitar que terceras personas puedan escuchar una comunicación y comprender su contenido.

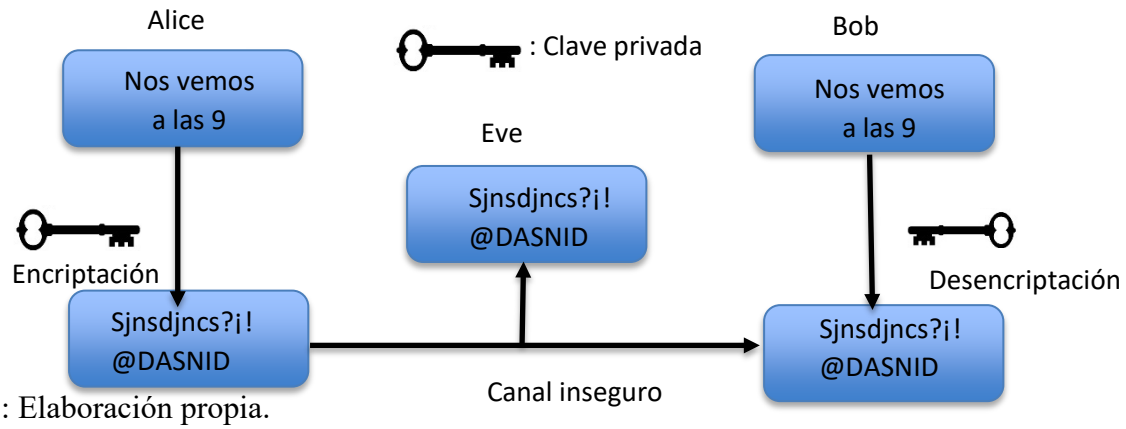
La criptografía cuántica ha hecho un aporte significativo a la industria de la criptografía. Las partes que se comunican entre sí pueden hacerlo gracias a los protocolos por la criptografía cuántica. Como resultado, proporciona una forma de determinar si se está llevando a cabo una escucha confidencial sobre una comunicación encriptada. Desde de ahora, nombres Alice, Bob y Eve se utilizarán a fin de describir al remitente, receptor y al destinatario por medio de atención los contenidos secretos.

En ejemplos de criptografía y comunicaciones, los nombres Alice y Bob se utilizan tradicionalmente en lugar de las letras A y B para referirse a los participantes de una comunicación entre dos puntos. El nombre Eve proviene de la palabra inglesa Evesdropper, que significa "quien escucha en secreto".

Tanto los algoritmos de clave privada y de clave pública son las dos categorías más comunes de algoritmos de encriptación. Los algoritmos de clave pública también se conocen como algoritmos antisimétricos. Los algoritmos de encriptación simétricos o convencionales son otros nombres para los algoritmos de clave privada.

Modelo de Criptografía Convencional o de Clave Privada: En el modelo convencional, el mensaje original que es comprensible se convierte en un mensaje aparentemente aleatorio y sin sentido. Un algoritmo y una clave son los dos componentes del proceso de encriptación. Un valor que no está relacionado con el texto o el mensaje que se cifra se denomina clave. Dependiendo de la clave utilizada, el algoritmo generará una salida diferente para el mismo texto de entrada (Franchi, 2012). El mensaje puede ser transmitido una vez cifrado. La clave utilizada para la encriptación y un algoritmo de desencriptación pueden usarse para recuperar el mensaje original.

Figura 3 Criptografía Clase privada

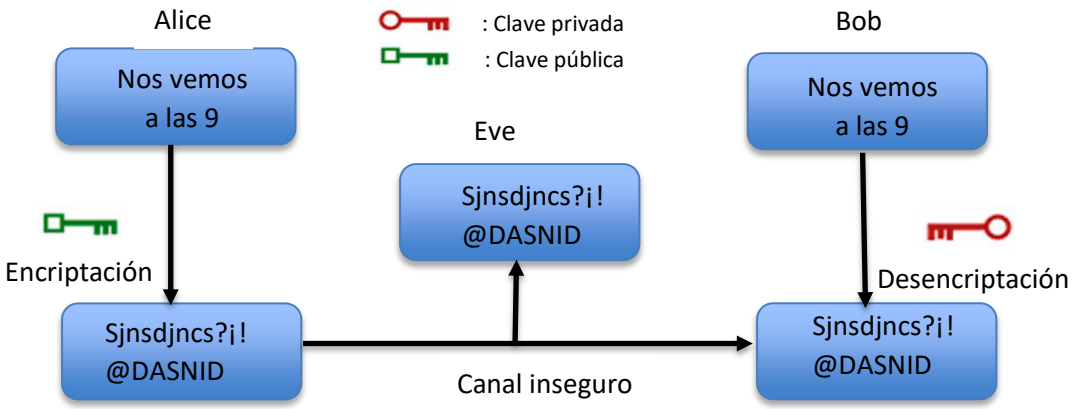


Fuente: Elaboración propia.

Modelo de Criptografía de Clave Pública

Los algoritmos de criptografía pública se basan en una clave de encriptación y una clave de desencriptación diferentes sin embargo relacionadas. Una característica de estos algoritmos es que es imposible distinguir entre la clave de desencriptación (clave privada) y la clave de encriptación (clave pública) y el algoritmo criptográfico (Franchi, 2012).
Es imposible de distinguir ya que el diseño cuidadoso y el uso de problemas matemáticamente difíciles lo que asegura que la seguridad del sistema no se vea comprometida al exponer la clave pública. Esto es fundamental para mantener la confidencialidad y la integridad de la información en la comunicación digital.

Figura 4 Criptografía Clave pública



Fuente: Elaboración propia.

Utilizando la figura 4 podemos exponer cada uno de los pasos necesarios para la encriptación con clave pública:

1. El proceso inicia cuando cada sistema crea un conjunto de claves, lo cual se genera un par de claves (clave pública y clave privada) mediante un algoritmo criptográfico. La clave pública se distribuye libremente, mientras que la clave privada se mantiene en secreto, para que puedan encriptar y desencriptar mensajes que remitan y recojan.
2. Luego, todos los sistemas recogen una clave de encriptación, también conocida como clave pública. La clave relacionada de desencriptación, también conocida como clave privada, se conserva en secreto.
3. Por ello, Si Alice desea enviar un mensaje a Bob, use la clave pública de Bob para encriptar el mensaje.

4. Y finalmente, Bob desencripta un mensaje con su clave privada. Debido a que Bob es el único que sabe su clave privada, nadie puede desencriptar el mensaje.

   Esto nos lleva a entender la diferencia entre la criptografía cuántica y la criptografía clásica, la criptografía cuántica representa una revolución en la seguridad de la información basada en principios cuánticos, mientras que la criptografía clásica se basa en problemas matemáticos complejos. Aunque la criptografía cuántica promete una seguridad sin precedentes, su implementación generalizada aún enfrenta desafíos técnicos y prácticos. La combinación de ambas tecnologías puede ser la clave para lograr comunicaciones verdaderamente seguras en el futuro.

CAPITULO 3

EL INTERNET CUÁNTICO COMO NUEVA ALTERNATIVA

Para poder comparar y definir cuál de estas dos tecnologías (internet clásico e internet cuántico) partiremos de analizar cada una de ellas, encontrando similitudes y diferencias.

3.1.Desarrollo histórico del internet clásico

El desarrollo del Internet clásico es un proceso fascinante que abarca más de medio siglo de innovación tecnológica, cambio cultural y evolución social. Esta historia comienza en las décadas de 1960 y 1970, cuando la idea de conectar computadoras para el intercambio de información comenzó a materializarse, y avanza hasta el mundo interconectado que conocemos hoy. Este resumen explora los hitos clave, los protagonistas y las implicaciones del Internet clásico, proporcionando referencias que permiten un análisis más profundo.

El origen del Internet se remonta a un proyecto de investigación del Departamento de Defensa de los Estados Unidos llamado ARPANET (Advanced Research Projects Agency Network). En 1969, ARPANET se convirtió en la primera red de computadoras interconectadas, permitiendo la comunicación entre computadoras en diferentes ubicaciones a través de un protocolo de conmutación de paquetes. Este método revolucionario consistía en dividir la información en pequeños paquetes que se enviaban por diferentes rutas y se ensamblaban nuevamente en su destino.

El diseño inicial de ARPANET fue conceptualizado por Vinton Cerf y Robert Kahn, quienes desarrollaron el protocolo TCP/IP en 1974. Cerf y Kahn propusieron un modelo que permitiría la interoperabilidad entre diferentes redes, sentando las bases para el Internet moderno (Cerf & Kahn, 1974).

En la década de 1970, el desarrollo y adopción del protocolo TCP/IP fue un hito crítico. En 1983, ARPANET adoptó oficialmente TCP/IP como su estándar de comunicación, lo que permitió que otras redes se unieran, creando un sistema de redes interconectadas. Esta transición marcó un cambio significativo, permitiendo la expansión más allá del ámbito académico y militar.

La comunidad de investigadores y académicos comenzó a organizarse en torno a la creación de redes, y en 1986 se lanzó NSFNET (National Science Foundation Network), una red que proporcionó la infraestructura necesaria para conectar universidades y centros de investigación. NSFNET desempeñó un papel fundamental en la expansión del acceso a Internet (Leiner *et al*., 2009).

El fin de la década de 1980 y el inicio de la década de 1990 marcaron el nacimiento de la World Wide Web, un sistema que facilitó la navegación y el acceso a información en línea. En 1989, el ingeniero Tim Berners-Lee propuso un sistema de gestión de información basado en hiperenlaces, y en 1991 lanzó la primera página web. Esto revolucionó la forma en que los usuarios interactuaban con la información en línea, haciendo que el acceso a la web fuera más amigable y accesible.

El primer navegador web gráfico, Mosaic, fue lanzado en 1993 por Marc Andreessen y Eric Bina. Mosaic hizo que la navegación por la web fuera intuitiva, tomando ventaja de elementos gráficos y de texto que permitían a los usuarios explorar contenido más fácilmente (Berners-Lee, 1999). Esta facilidad de uso y accesibilidad fueron factores clave que condujeron al crecimiento explosivo de Internet.

En 1995, las restricciones comerciales sobre el uso de Internet fueron levantadas, permitiendo su comercialización. Este cambio facilitó la creación de empresas en línea, llevando a la aparición de pioneros como Amazon y eBay. La combinación de tecnología accesible y un mercado potencialmente masivo generó una explosión de inversiones en empresas tecnológicas y en el desarrollo de infraestructuras (Friedman, 2005).

La burbuja de las .com surgió a finales de la década de 1990 con la especulación masiva en torno a las empresas de Internet. Las valoraciones de estas empresas se dispararon, pero muchos de ellos carecían de modelos de negocio sostenibles. En 2000, la burbuja estalló, provocando el colapso de muchas de estas empresas y una reevaluación del mercado tecnológico (Gordon, 1998).

A medida que el Internet evolucionaba, se introdujo el concepto de Web 2.0, que se centró en la interactividad, la colaboración y el contenido generado por el usuario. Plataformas como YouTube, Facebook, y Wikipedia surgieron, permitiendo a los usuarios no solo consumir contenido, sino también crearlo y compartirlo.

Este cambio en el enfoque de la web transformó la manera en que las personas se comunicaban y compartían información. La creación de redes sociales facilitó nuevas formas de conexión y participación, cambiando radicalmente la forma en que interactuamos en línea (Tapscott & Williams, 2006).

La llegada de los smartphones a finales de la década de 2000, comenzando con el iPhone en 2007, transformó el acceso a Internet. A partir de entonces, la conectividad se volvió omnipresente, permitiendo que la información estuviera disponible en cualquier lugar y en cualquier momento. Esto modificó no solo cómo se accedía a la web, sino también cómo se interactuaba con el contenido y entre usuarios (O'Reilly, 2007).

El concepto de Internet de las cosas (IoT) comenzó a tomar forma, conectando dispositivos y electrodomésticos a una red para facilitar el intercambio de información. Este avance planteó nuevas oportunidades y desafíos, como la gestión de datos y la privacidad del usuario (Zittrain, 2009).

A medida que Internet ha crecido, también lo han hecho las preocupaciones sobre ciberseguridad, privacidad y brecha digital. Los ataques cibernéticos y las violaciones de datos han llevado a una creciente necesidad de políticas y regulaciones para proteger la información personal.

La brecha digital, que se refiere a las desigualdades en el acceso a Internet, continúa siendo un desafío importante. A pesar de los avances significativos, muchas comunidades y poblaciones siguen sin tener acceso adecuado o asequible a la tecnología (Bohman, 2010).

El desarrollo del Internet seguirá avanzando con la integración de nuevas tecnologías, como la inteligencia artificial, la realidad aumentada entre otro como incluso los avances del internet cuántico. Sin embargo, es esencial abordar los desafíos existentes, como la ética en el uso de datos y el acceso equitativo para garantizar que Internet continúe siendo una herramienta valiosa y enriquecedora. Por ellos, a medida que la tecnología continúa evolucionando, es fundamental reflexionar sobre cómo modelar un Internet que sea inclusivo y seguro, aprovechando su potencial para generar un impacto positivo en la sociedad.

Por lo tanto, el desarrollo histórico del Internet clásico es un viaje que abarca más de cinco décadas, donde la innovación constante y la adaptabilidad han transformado la comunicación, la cultura y la economía global. Desde los pioneros de ARPANET hasta la explosión de la

World Wide Web y más allá, el Internet ha resonado a través de generaciones, moldeando la forma en que nos conectamos y compartimos información.

3.2.El internet clásico en la actualidad

Actualmente, el internet clásico es un sistema global de redes de computadoras conectadas. De esta manera, la enunciación más conocida de Internet es similar a una red. Tal vez debido a la idea generalizada de que Internet es una especie de nube alejada y omnipresente desde el cielo, a menudo se ignora su dimensión física fundamental para estudiarla. Internet también llamada red de computadoras asi como otros dispositivos conectados por cables en todo el mundo. Como resultado, se compone de una gran cantidad de dispositivos que realizan una amplia gama de funciones (como usar tu computadora en casa para consultar sitios web, o servidores que alojan sitios web de noticias a los que consultas constantemente, entre otros), ubicados en todo el mundo y conectados a través de una variedad de medios (cables de fibra óptica, satélites, entre otros).

La comunicación entre computadoras se lleva a cabo a través del conjunto de protocolos TCP/IP ampliamente utilizado para la interoperabilidad en redes, que son directrices las cuales establecen la manera de transportarse contenidos e información a través del internet.

Si no utilizan las mismas reglas o protocolos para comunicarse, las computadoras conectadas a Internet no podrían comunicarse ni intercambiar información. Un proveedor de acceso a internet (ISP), cierta organización cuyo principal objetivo es facilitar la comunicación, es responsable de la conexión a esta inmensa red llamada internet. Para lograrlo, el distribuidor determina un número único en la red, lo que nos permite identificarnos cuando accedemos a la red. Este código único que se le asigna a nuestra computadora se conoce como IP, y no puede ser usado por otra computadora en la red al mismo tiempo. El cual es similar a nuestro nombre, apellido y dirección de computadora.

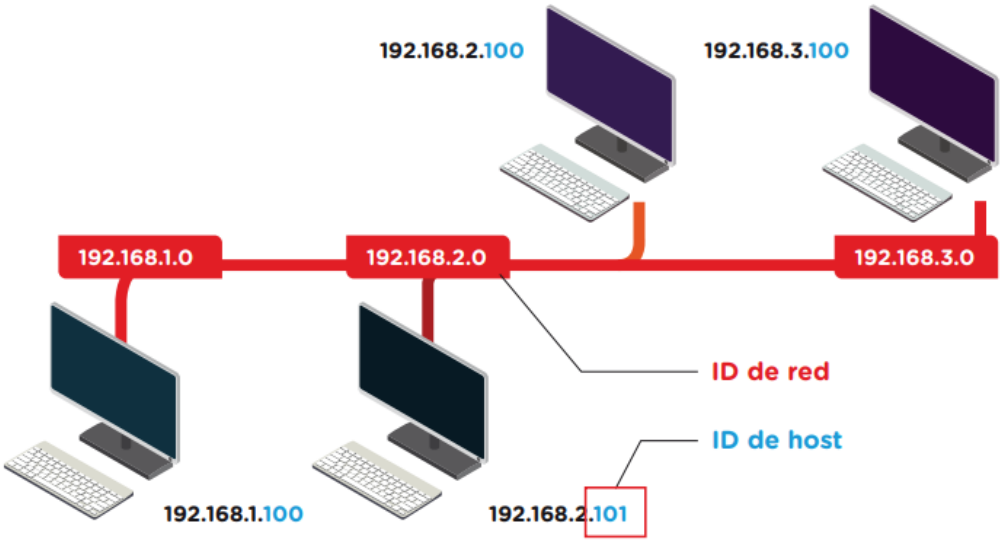
Es importante conocer que, dicho código numérico que identifica y ubica una computadora se conoce como IP de la computadora. El único código el cual identifica la computadora conectada a la red global se conoce como IP. Permite que las computadoras se identifiquen y se comuniquen entre sí.

En un IP cada uno de los cuatro números que componen el protocolo de Internet, alejados por puntos, obtiene valores que van desde 0 hasta 255 los cuales van a tener un significado único. El primer número de la dirección IP de una computadora identifica la red de internet, el

segundo número identifica la computadora, el tercer número representa a la red de computadoras más reducida y el cuarto número representa la computadora en sí.

Debido a la gran cantidad de computadoras conectadas a la red, el protocolo Internet Protocol (IP) se clasifica en clases debido a su complejidad. Por ejemplo, la clase A recibe el primer número se utiliza para identificar la red, mientras que los tres últimos se reservan para asignarlos al host o servidores de internet.

Figura 5 IP Clase A



Fuente: Currículos Exploratorios en TIC, 2024.

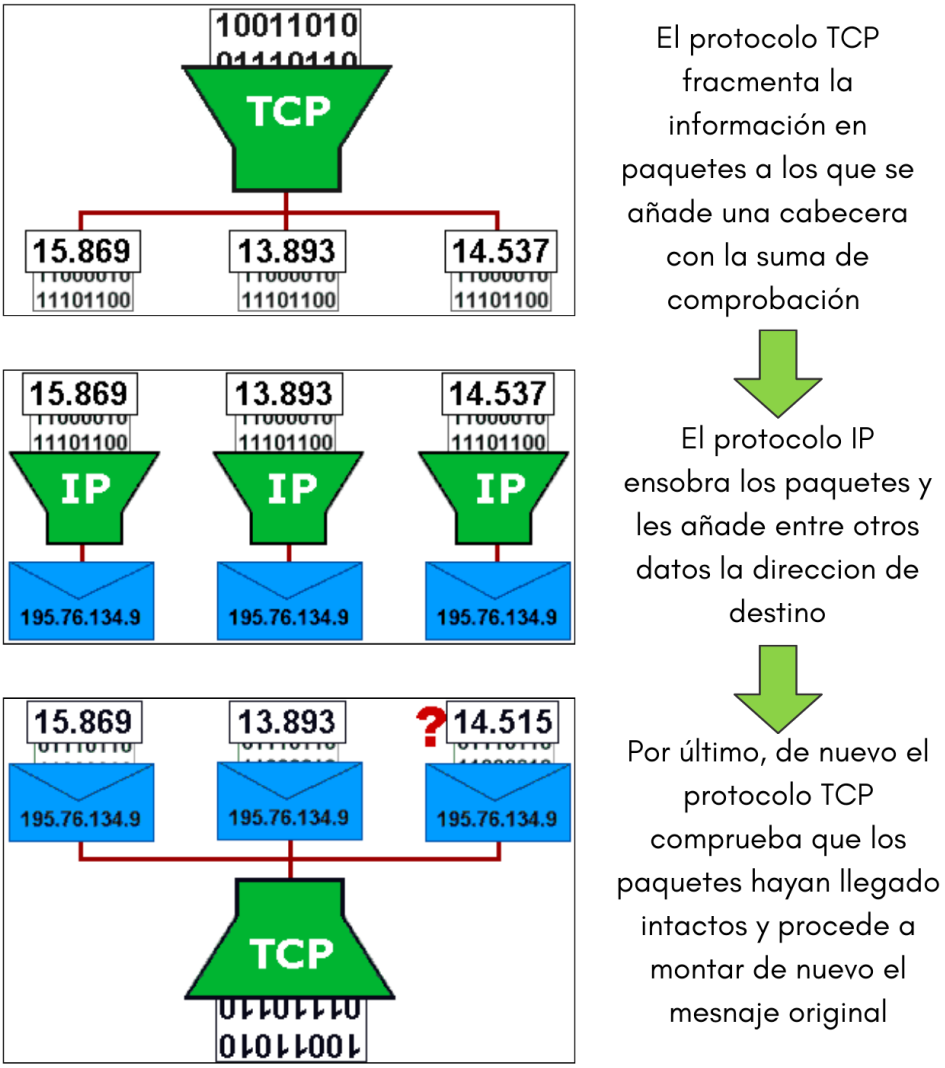
Los datos y la información que deseamos remitir por Internet deberán convertirse en códigos para que así logren viajar por cables u ondas electromagnéticas. Para enviar información, es necesario convertir las señales digitales de la computadora en analógicas y recibir información, los datos analógicos deben convertirse en digitales.

Hasta hace poco, el módem (modulador/demodulador) se encargaba de esta conversión, pero en la actualidad se emplea el enrutador o enrutador, el cual muestra un algoritmo de rendimiento superior en la toma de decisiones porque, asi como realizar ciertas actividades del módem, también puede administrar decidir por qué ruta enviar, qué enviar y a dónde enviar, es decir, los datos que enviamos o recibimos.

También es crucial conocer sobre el protocolo TCP, que son pautas de cómo debe enviarse la información, este TCP puede fragmentar información en paquetes que se deben reensamblar al llegar al destino final para reconstruir la información completa. Por lo tanto, estándares o

protocolos especifican a manera de enviar, unir y segmentar la información en paquetes de datos. En este proceso, el protocolo TCP añade una cabecera a cada segmento de datos el cual contiene una variedad de datos, incluido el orden en que deben unirse. El protocolo TCP puede incluir datos y dirección de destino en cada paquete que se envía en forma de sobre. El protocolo TCP se activa nuevamente, realiza una nueva comprobación y lo compara. cuando llegan los paquetes, con el paquete original. Se requiere un nuevo desplazamiento del paquete desde el origen si cualquiera de los paquetes no coincide y muestra desaparición de información en el trayecto. El TCP une los paquetes de información después de verificar que son auténticos y crea el mensaje original.

Figura 6 Protocolos TCP/IP



Fuente: Área tecnología, 2024. Elaboración propia.

Como resultado, llegamos a los servidores, que son computadoras configuradas para el servicio al usuario. Estos servidores son de amplia capacidad, tanto como almacenar cualquier tipo de información. Las computadoras especiales tienen más capacidad de almacenamiento que las computadoras normales y pueden funcionar las 24 horas del día, los 365 días del año.

Recordemos, la unidad de información más pequeña es un byte, que solo puede ser un valor de 0 o 1. Por lo tanto, un solo bit será suficiente para almacenar dos valores. Necesitaremos dos bits si queremos almacenar cuatro valores, y los valores almacenados serán 00, 01, 10 y 11. En general, podemos representar 2 elevado a n valores con n bits. Por otro lado, es importante recordar que un byte está compuesto por ocho bits. Como resultado, un byte puede almacenar hasta 256 valores diferentes, ya que se corresponde con 2^8. En cuanto a la capacidad de almacenamiento de un servidor típico, puede oscilar entre 1 y 2 terabytes, pero hay servidores que pueden almacenar hasta 1000 terabytes, lo que es equivalente a un petabyte. Esta información fue proporcionada por Pastor Collado y Elias Vila en 2017.

Tabla 1 Resumen de la conversión de petabytes en todas las unidades comunes

Volumen de datos	En petabyte	En byte
1 bit	1/9 007 199 254 740 992	1/8
1 nibble	1/2 251 799 813 685 248	1/2
1 byte (B)	1/1 125 899 906 842 624	1
1 kilobyte (KB)	1/1 099 511 627 776	1024
1 megabyte (MB)	1/1 073 741 824	1024^2
1 gigabyte (GB)	1/1 048 576	10243
1 terabyte (TB)	1/1024	1024^4
1 petabyte (PB)	1	1024^5
1 exabyte (GB)	1024	1024^6
1 zettabyte (ZB)	1 048 576	1024^7
1 yottabyte (YB)	1 073 741 824	1024^8
1 brontobyte (BB)	1 099 511 627 776	1024^9

Fuente: Elaboración propia.

3.3.Desarrollo Histórico del Internet cuántico

El concepto de internet cuántico no puede atribuirse a una sola persona específica, ya que es el resultado de la suma de ideas y teorías en múltiples campos científicos y tecnológicos relacionados con la física cuántica, la informática y las comunicaciones.

Sin embargo, según Richard Primera (2004) investigadores y científicos como Richard Feynman, quien propuso el uso de fenómenos cuánticos para cálculos computacionales, y otros científicos que han trabajado en la teoría de la información cuántica, como David Deutsch y Charles Bennett. Estas contribuciones han sido fundamentales en el desarrollo y la exploración de los principios subyacentes al internet cuántico.

Es asi que el físico Alemán Max Planck quien se notó obligado a simplificar para presentar resultados experimentales en relación con el espectro del cuerpo negro, las modificaciones de energía entre átomos y radiación. Posteriormente afirmó que fue "como un acto de desesperación". Poco después se presentó ante la Sociedad Alemana de Física exactamente el 14 de diciembre del año 1900, en el que introdujo tanto la constante universal *h* como el término quantum en la física. Poco tiempo después, dentro de su obra Agnus Mirabilis, diseñado por Albert Einstein en 1905, sugiere que los gránulos indivisibles de valor *hn* concentran la energía de una sola luz de frecuencia *n*.

Veinte años más tarde, estos quanta o paquetes de luz se denominarían fotones, porque la mecánica cuántica empezó con problemas de cuantización de la luz/del campo eletromagnético, es importante mencionar que no solamente los fotones son cuantizados, sino que para el problema del efecto fotoeléctrico los quanta son fotones. Cabe resaltar que estos trabajos iniciales simplemente obligaban a reconocer que la energía ocasionalmente surgía en embalajes discretos, sin embargo, no pudo ser incorporada a una comprensión de la naturaleza basada en la física. La teoría experimentó un gran avance cuando Heinsenberg y Schrödinger realizaron contribuciones para el desarrollo de la teoría y su fundamentación. La hipótesis cuántica establece que la energía luminosa no se emite ni se absorbe de manera continua, sino en pequeños paquetes discretos llamados "cuantos". Siempre, independientemente de su tamaño, las partículas no pueden ocupar un solo punto del espacio-tiempo, sino que se extienden a lo largo de una trayectoria en la que se encuentran en diferentes puntos a lo largo del tiempo. Este principio refleja la naturaleza continua y cuadridimensional del espacio-temporal. Se argumenta en la misma línea de pensamiento como "hipótesis granular" el cual sugiere que hay ciertos valores que son prohibidos para las medidas cuantitativas en

distribuciones de materia, debido a que la materia no puede dividirse indefinidamente y debe ajustarse a un "cuanto mínimo". Esto implica que cualquier medida total en dicho contexto debe ser un múltiplo de esta unidad fundamental. Por lo tanto, hay valores que no están permitidos para medir las distribuciones materiales y, por lo tanto, sus magnitudes teóricas (energía, impulso, etc.). Es necesario tener una cantidad mínima de energía, impulso y otros elementos, y sus valores para un sistema deben ser superiores a esa cantidad mínima.

Asimismo, la cuantización, el principio de incertidumbre, la superposición cuántica, el tuneleo, el entrelazamiento y la decoherencia valieron como fundamento para el desarrollo de la mecánica cuántica (Primera, 2004). La visión de la realidad nunca sería como antes si se rompiera el antiguo prohibición y se liberara la aparición de la discretización.

Richard Primera (2004) también indica que, antes de la segunda mitad del siglo XX, nueve científicos destacados como Niels Bohr (1913), Einstein (1905) y Planck (1900), fueron continuados por Wolfgang Pauli (1925), Erwin Schrödinger (1926), Werner Karl Heisenberg (1924), Louis (Víctor Pierre Raymond) de Broglie (1923), Paul (Adrien Maurice) Dirac (1928), Max Born (1926). La interpretación de Copenhaguen representó el punto más alto de los esfuerzos creativos de Schrödinger, Heisenberg y Dirac, fue una estructuración matemáticamente consistente de la mecánica cuántica, pero cubierta de un cierto halo de misterio. Si bien Einstein se oponía firmemente a la mecánica cuántica debido a que la consideraba incompleta, su uso generaba paradojas fascinantes como por ejemplo la del gato de Schrödinger o la paradoja de Rosen, Podolski y Einstein, las cuales demostraban la disconformidad de los fundamentos de la mecánica cuántica fundamentales de la naturaleza física, al igual que la causalidad y la realidad. En lugar de física cuántica, se desarrollaron varias teorías denominadas teorías de variables ocultas, las cuales buscan asegurar que, si se descubrieran los valores de estas inconstantes adicionales, estaría claro y no habría inseguridades ni consecuencias probabilísticos.

Aunque la gente no tenía mucho interés en la década de los 60, en el desarrollo de la mecánica cuántica, John Bell, un físico del CERN (Ginebra), logró cambiar radicalmente esta percepción. Bell notó que las predicciones derivadas de la teoría de que existen variables ocultas eran diferentes de las obtenidas utilizando la mecánica cuántica. En términos simples, si las predicciones de la mecánica cuántica superan estas desigualdades, se puede concluir que las teorías de variables ocultas locales están incorrectas. Esto está referido a las discrepancias de físico Bell que llevaron preguntas acerca de los fundamentos de la mecánica cuántica a partir de la opinión filosófica hasta la evidencia física del ensayo. Sin embargo, esta tecnología

no fue capaz de realizar estos experimentos hasta la década de los 80. En Orsay (Francia), Alain Aspect ganó demostró que las desigualdades de Bell son verdaderas experimentalmente y, con esto, la mecánica cuántica no es una teoría incompleta, la cual implica que el argumento EPR se ha destruido por siempre. Desde entonces, los experimentos ficticios que habían sido utilizados por Heisenberg o Einstein para justificar sus teorías estaban dentro del ámbito de las pruebas reales en la década de los noventa, viene siendo marcada por la expansión en dicho campo emergente donde estos experimentos intrigantes se han llevado a cabo despertando el interés público. Otro ejemplo, es uwn artículo de la revista Science hablaba acerca de la prueba de traslación llevado a cabo mediante el físico Nicolas Gisin y sus colaboradores en la Universidad de Ginebra (Gisin & Fasel, 1998).

En los años 2000, se llevaron a cabo los primeros experimentos de distribución de clave cuántica a larga distancia (QKD). Estos experimentos establecieron récords en la transmisión segura de información cuántica a través de fibra óptica. De igual manera, Ignacio Cirac y Peter Zoller sugieren técnicas para la creación y alteración de estados entrelazados cuánticamente, los cuales son cruciales para la teleportación cuántica y la transmisión de información cuántica a larga distancia.

Los algoritmos cuánticos fundamentales fueron desarrollados por Peter Shor y Lov Grover en la década de 1990. El algoritmo de factorización de números enteros llamado algoritmo de Shor, desarrollado por Peter Shor, la ventaja teórica de los computadores cuánticos, como demuestra el algoritmo de Shor, radica en su capacidad para resolver problemas complejos de factorización de manera exponencialmente más eficiente que los computadores clásicos. Esto plantea un desafío significativo para la criptoseguridad actual, y es un motivo por el cual se están investigando nuevas formas de criptografía, como la criptografía cuántica y los esquemas post-cuánticos, que sean resistentes a ataques cuánticos. El algoritmo de búsqueda cuántica, que también demostró las capacidades distintivas de los computadores cuánticos, ofrece una mejora cuadrática en la búsqueda de elementos no estructurados en bases de datos no ordenadas.

Los esfuerzos para integrar tecnologías cuánticas con infraestructuras de comunicaciones existentes y la creación de arquitecturas de redes cuánticas se intensificieron en la década de 2010. Los físicos teóricos Ignacio Cirac y Peter Zoller han aportado mucho al ámbito de la informática y las comunicaciones cuánticas, proponiendo métodos para el entrelazamiento y la teleportación cuánticas, que son esenciales para el internet cuántico.

El término “internet cuántico” hace referencia a una posibilidad de transformación del internet actual mediante el uso de conceptos de la física cuántica. Sin embargo, el internet cuántico en su forma completa y funcional aún no existe. Su origen conceptual se remonta a conceptos teóricos exploratorios sobre cómo los fenómenos cuánticos podrían optimizar la eficacia y la seguridad de las comunicaciones en red.

3.4.El internet cuántico en la actualidad

El concepto de internet cuántico ha avanzado significativamente en la última década, con desarrollos tecnológicos que prometen transformar la manera en que transmitimos y aseguramos la información. Basado en principios de la mecánica cuántica, este nuevo paradigma de comunicación está diseñado para ofrecer una mayor seguridad y mejorar la velocidad de transmisión de datos. A continuación, se exploran los hitos más importantes en el desarrollo del internet cuántico desde 2013 hasta 2023, resaltando los puntos importantes y desafíos que aún deben ser superados.

Desde 2013, la investigación en comunicaciones cuánticas ha comenzado a consolidarse como un campo de estudio esencial. Se hayan desarrollado conceptos fundamentales como la distribución de claves cuánticas (QKD, por sus siglas en inglés) y la teletransportación cuántica que son esenciales para la infraestructura del internet cuántico (Gisin *et al*., 2002). Estos avances teóricos han sido seguidos por experimentos prácticos que demuestran la viabilidad de estas tecnologías, estableciendo una base sólida para la creación de redes cuánticas.

Uno de los desarrollos más notables fue el lanzamiento del satélite cuántico Micius por parte del equipo de investigación chino en 2016. Este satélite ha logrado estandarizar la distribución de claves cuánticas entre diferentes puntos en la Tierra, estableciendo récords de distancia en la transmisión de información cuántica. En 2017, se demostró la capacidad de Micius para llevar a cabo QKD a una distancia de 4,600 km, un hito que subraya el potencial de la comunicación cuántica en la infraestructura global (Liao *et al*., 2017).

En Europa, el proyecto Quantum Internet alliance (QIA), lanzado en 2019, busca conectar varias ciudades para desarrollar una red de internet cuántico. Este esfuerzo une a instituciones académicas y empresas en un marco de colaboración para investigar cómo interconectar nodos cuánticos y fomentar la interoperabilidad entre redes cuánticas y clásicas. Se están realizando

pruebas en diversas ciudades, incluyendo Delft, Ámsterdam y La Haya, donde se han desplegado conexiones cuánticas (Quantum Internet alliance, 2020).

Respecto a la implementaciones y prototipos, instituciones académicas y corporaciones de tecnología, como IBM y Google, han comenzado a desarrollar prototipos de redes aquíétaire cuántica. En 2020, IBM lanzó su plan para construir una red cuántica en la que se puedan conectar múltiples dispositivos cuánticos mediante nodos específicos. Además, la compañía ha trabajado en la mejora de sus computadoras cuánticas, que son esenciales para el funcionamiento de las redes cuánticas (Caleffi, 2021). Este enfoque ha promovido el desarrollo de software de simulación que puede ayudar en la creación de algoritmos para la corrección de errores y la optimización de las operaciones en una red cuántica.

Con relación a los desafíos en el Desarrollo del Internet Cuántico y pesar de los avances, varios desafíos técnicos siguen obstaculizando el desarrollo del internet cuántico. La decoherencia cuántica es uno de los problemas principales, ya que se refiere a la pérdida de información cuántica debido a interacciones no deseadas con el entorno. Mantener la coherencia cuántica durante la transmisión a largas distancias es fundamental para la fiabilidad de una red cuántica (Pirandola *et al*., 2015). Los investigadores están explorando nuevas técnicas para proteger la información cuántica, incluidas estrategias de corrección de errores cuánticos que podrían hacer más robustas las comunicaciones cuánticas.

Otro desafío es la escalabilidad de las redes cuánticas. Si bien se han establecido comunicaciones en distancias relativamente largas, replicar esta infraestructura a gran escala requiere un diseño eficiente de nodos cuánticos que puedan comunicarse de manera efectiva en toda la red, además de tecnologías de almacenamiento cuántico capaces de retener información hasta que sea necesario (Matsuo *et al*., 2020).

Sobre el impacto futuro y aplicaciones potenciales podemos decir que, a medida que la investigación y los desarrollos continúan, las aplicaciones del internet cuántico se vislumbran amplias, desde la criptografía cuántica, que promete un nivel de seguridad incomparado, hasta la mejora en la simulación de materiales en la computación cuántica. La posibilidad de realizar cálculos altamente paralelizados a través de redes cuánticas abre la puerta a innovaciones en áreas como la inteligencia artificial y el diseño de fármacos (Kjaergaard *et al*., 2020).

El internet cuántico también tiene el potencial de crear una nueva economía digital, donde los protocolos de confianza y seguridad se redefinan, fomentando así un entorno donde la privacidad de los datos sea prioritaria. Las implicaciones para la defensa y la seguridad

nacional también son significativas, ya que las capacidades cuánticas podrían ofrecer nuevas formas de proteger sistemas críticos.

3.4.1. Arquitectura de una computadora cuántica

Con ciertas características específicas de la arquitectura de las computadoras cuánticas es similar a la de una computadora tradicional. Se sugiere como estructura para la computación cuántica que incluye ALU cuántica (el cual se refiere a la unidad aritmética lógica que opera dentro de un sistema de computación cuántica), memoria cuántica y un planificador dinámico. Transformar las irregularidades de los componentes cruciales del diseño de una arquitectura cuántica. En la actualidad, se conoce la forma en que los sistemas cuánticos pueden leer y escribir información mediante procesos de escritura que involucran la manipulación de la energía necesaria para escribir un 0 o un 1; además, se debe tener en consideración la entropía cuántica que se refiere a se refiere a la medida de incertidumbre o desorden en los sistemas cuánticos utilizados para la transmisión de información y es crucial para evaluar la seguridad y eficacia del intercambio de datos a través de redes cuánticas, ya que ayuda a entender cómo se gestionan y se protegen las informaciones en un sistema cuántico.

Es importante destacar que la corrección de errores es crucial, como cualesquiera las aplicaciones de gestión y registro de datos ruidosos, habría que alterar componentes de manera aleatoria. Las tecnologías convencionales, corrección de errores, requieren una evaluación de bits para determinan que se incorrectos, causaría decoherencia a una computadora cuántica, dicha decoherencia es el procedimiento por el cual se pierde la coherencia cuántica.

La función principal de la ALU cuántica es la corrección de errores y la ejecución de operaciones cuánticas. Anteriormente se usaba una compuerta lógica, prepara los datos mediante una serie de evoluciones cuánticas fundamentales, que incluyen: X, NOT cuántico, NOT controlado (CNOT); I, Identidad (I, NOP cuántico), Z, logra cambiar los signos de las amplitudes, Y = XZ, S que es la rotación por $\pi/4$, T el cual es la rotación por $\pi/8$ y la puerta Hadamard que es un operador que transforma un estado básico de un qubit en una superposición. Este último se conoce como la raíz cuadrada de la transformada de Fourier en el contexto de un qubit, ya que permite que el qubit pase de un estado definido a un estado donde tiene probabilidades de ser observado en múltiples estados al mismo tiempo. Esto es fundamental para el procesamiento paralelo de la información en computadoras cuánticas (Primera, 2004).

Dentro de los computadores tradicionales, existen puertas lógicas que resuelven los datos con componentes no lineales que se derivan de tecnología semiconductora, como dispositivos transistores de computadores. Sin embargo, en computadores cuánticos, las compuertas lógicas se obtienen mediante interacciones no lineales entre magnitudes cuánticas. Aunque todas las puertas clásicas tienen una contraparte, existen entradas cuánticas exóticas que carecen de contraparte clásica. Una entrada pequeña no tradicional cNOT, que es una compuerta cuántica de 2 qubits.

Actualmente se están construyendo uno de los principales componentes de los que será el internet cuántico y son las "entradas" prácticos de cNOT de dos qubits las cuales se están manipulando métodos simples para corregir los errores. Es importante recalcar que, para la construcción de una computadora cuántica, se deben solucionar numerosos inconvenientes, incluida la selección también llamados tecnologías físicas que exhiben qubits, el manejo de estas puertas cuánticas, el control de fallas y el suceso de acrecentar la capacidad de la computadora cuántica solucionar problemas de múltiples tipos (Primera, 2004).

Con el fin de satisfacer estas exigencias, se están estudiando una amplia gama de métodos físicos, las cuales se organizan en función a sus características como también interacciones, tal como lo menciona Richard Primera (2004) y como se muestra a continuación:

Los dipolos magnéticos de las moléculas se controlan con resonancia magnética nuclear. Usando el algoritmo de Deutsch, se lograron avances experimentales notables. Cory desarrolló una estrategia para corregir defectos en el proceso debido a variaciones en el campo magnético, empleando un método de tres qubits con tricloroetileno y alanina. En 2001, el Dr. Wei implementó puertas de control y de raíz cuadrada con siete qubits, representando los cuatro carbonos y tres hidrógenos del ácido crotónico.

Aplicaciones de iones extremadamente fríos que utilizan protectores iónicos y lentes láser, en el National Institute of Standards and Technology (Colorado), se utilizó esta técnica para construir la primera puerta cNOT cuántica. Los experimentos utilizaron el ion Be^{+} tiene dos niveles de tierra ultrafinos como qubits de imágenes, los dos primeros modos de vibración, también conocidos como fonon, representaron el registro de qubit. El mismo sistema tiene dos qubits de la puerta cNOT que se encuentran en diferentes grados de libertad. Monroe logra que la puerta funcione correctamente en un 90%. En 1995, Cirac y Zoller propusieron el uso de trampas de iones lineales para resolver el problema de escala. Hasta el momento, a pesar de un gran esfuerzo, no se ha logrado implementar ninguna puerta cNOT a través de estos

sistemas. Sin embargo, existen trampas para controlar conjuntos de iones como los de Ca^{+}. Respecto a la Polarización de los fotones o algún método que permita incorporar fases globales, Primera (2004) nos dice que es posible utilizar dos enfoques principales: el enfoque de los "qubits voladores" desarrollado por el equipo de Kimble en Caltech, y el montaje realizado por Haroche de la École Normale Supérieure de París.

Para llevar a cabo una lógica cuántica, los sistemas de fase sólida aprovechan la coherencia macroscópica de los pares de Cooper mediante una heterounión Josephson. Aunque se han creado puertas cNOT experimentales que utilizan dos qubits y se han aplicado técnicas básicas de corrección de errores, no se espera que los ordenadores cuánticos puedan realizar tareas significativas en el corto plazo (Primera, 2004).

Cabe resaltar que toda esta arquitectura de la llamada computadora cuántica es y será fundamental para lograr las metas planteadas y resolver los obstáculos que hasta ahora se han presentado en los distintos estudios acerca del tema. Sin embargo, es también importante indicar que aún falta mucho tiempo para lograr su uso masivo debido a las características y por ende el costo que representa su elaboración.

3.4.2. El internet cuántico y sus Casos de éxito hasta la actualidad

El desarrollo del internet cuántico representa una de las fronteras más avanzadas en la tecnología de la información, prometiendo una seguridad sin precedentes y velocidades de transmisión de datos significativamente mayores. A medida que diferentes regiones del mundo compiten en este campo, China, Estados Unidos y Europa están realizando experimentos fundamentales que podrían definir el futuro de las comunicaciones cuánticas.

Caso China: China ya es uno de los países con mayores avances de tecnología a nivel mundial y por ellos está invirtiendo una cantidad significativa de recursos en el avance de las comunicaciones cuánticas. Tal como lo menciona Juan Carlos Lopez (2023), en el año 2017, científicos de la Universidad de Ciencia y Tecnología de China, así como de la Academia de Ciencias de China lograron enviar pares de fotones entrelazados a una distancia de más de 1200 km a través de un satélite. Hasta ese año, todos los intentos para lograr entrelazar partículas, es decir una forma de “vincularlas” de forma cuántica a distancia, se limitaban a 100 km o incluso menor distancia, esto sucedía debido a que el entrelazamiento se va

debilitando a medida que las partículas se transmiten a través de los cables de fibras ópticas o espacios abiertos terrestres.

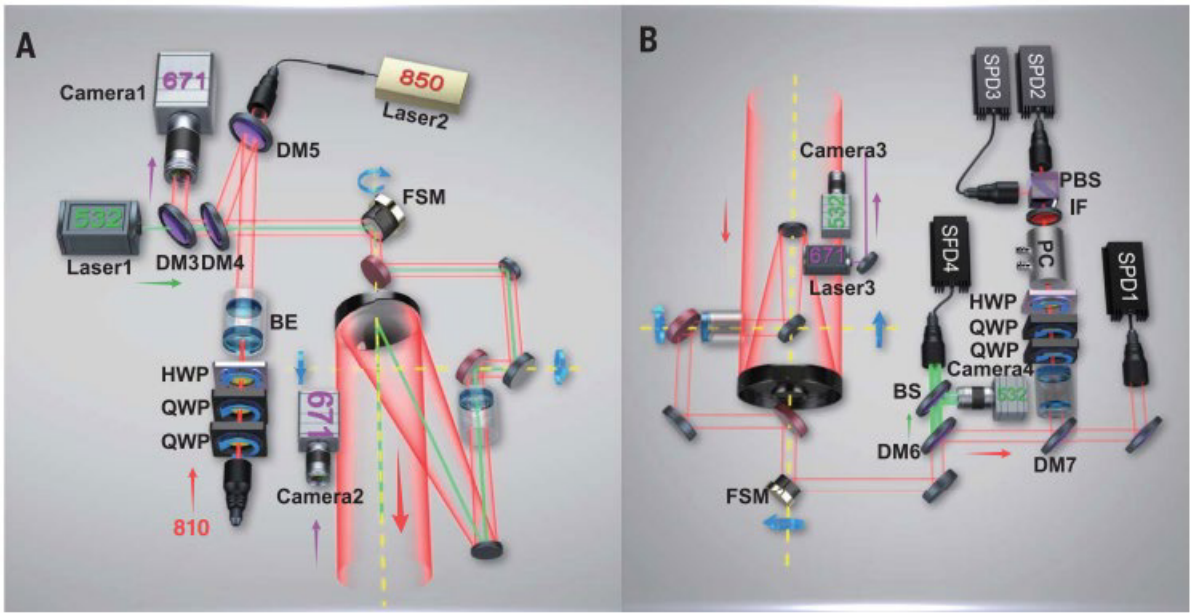
Del mismo modo, lo que conocemos como línea de transmisión se divide en segmentos más pequeños, lo que permite a los científicos como Yin *et al* (2017) intercambiar, depurar y acopiar muchos datos cuánticos a lo largo de la fibra en repetidas ocasiones, lo que es una forma de superar este problema. Ademas, existen métodos alternativos para establecer redes cuánticas a nivel mundial que utilizan láseres y tecnologías basadas en satélites. Uno de los ejemplos más destacados es el trabajo del grupo de científicos chinos liderado por el investigador Yin, que ha logrado implementar estas técnicas efectivamente para desarrollar redes de telecomunicación cuántica tanto terrestres como espaciales.

Los autores de dichos estudios han usado "el satélite Micius o Mozi, bautizado en honor a un filósofo y científico chino del siglo quinto a.C. para su estudio. La nave, que se lanzó en el año 2016, la cual estuvo equipada con herramientas cuánticas y tecnologías muy especializadas" (Sacristán, 2017).

Según autores como López (2022) la comunicación a través del satélite se llevó a cabo utilizando tres estaciones en tierra ubicadas en diferentes: Nanshan en la ciudad de Urumqi, Delingha en Qinghai y el Observatorio Gaomeigu en Lijiang, todos ellos lugares de China (López J. C., 2022). El récord de entrelazamiento cuántico se estableció entre Delingha y el Observatorio Gaomeigu, que están alejadas una de la otra por una distancia de 1203 km. Del mismo modo, la distancia entre las estaciones que se encuentran en tierra y el satélite en órbita fue de entre 500 y 2000 km.

Destaca que el trabajo ha demostrado que es factible obtener pares de fotones entrelazados a distancias nunca antes alcanzadas. Esto se logra transmitiendo pares entrelazados desde un satélite, lo que posibilita su propagación en un espacio muy abierto, reduciendo las conexiones que podrían comprometer la coherencia." (López E. , 2017).

Figura 7 Los transmisores, receptores y rendimiento del APT



Fuente: Satellite-based entanglement distribution over 1200 kilometers. Yin *et al*., 2017.

En la figura 7 se muestra (A) El sistema utiliza un haz de fotones entrelazados de 810 nm, que se combina con un láser infrarrojo pulsado de 850 nm para sincronización y un láser verde de 532 nm para seguimiento, enviado desde un telescopio de 8x. La compensación de polarización se realiza con dos placas de onda cuarteadas motorizadas y una placa de onda half controladas de manera remota. Se implementan un espejo de dirección rápida y una plataforma giratoria de dos ejes para el seguimiento (B) En el receptor en Delingha, se utilizan sistemas similares al del satélite, con láseres separados del fotón de señal y detectores de fotón único para el análisis de polarización (Yin *et al*, 2017).

Además, en 2021, un equipo de investigadores en China mostró la capacidad de realizar teleportación cuántica entre tres nodos de la red, lo que es un paso significativo hacia el establecimiento de un internet cuántico funcional (Pan *et al*., 2021). Estos avances no solo destacan la capacidad del país para innovar en este campo, sino que también plantean nuevas preguntas sobre la gobernanza y la seguridad en el uso de tecnologías cuánticas.

Aunque este último no solo se encuentra entre los progresos más notables en este ámbito hasta el momento, en el año 2022, un segundo grupo de científicos chinos logró realizar una comunicación cuántica segura y directa (QSDC) a una distancia de 102,2 km.

Los objetivos de estos experimentos son desarrollar la tecnología necesaria para permitir las comunicaciones cuánticas a larga distancia, que son fundamentales para la creación de la internet cuántica.

Caso Estados unidos: Otro principal país en cuanto a tecnología es Estados Unidos, donde en julio de 2020, United States Department of Energy o conocido como DOE reveló su plan para promover el progreso tecnológico necesaria para establecer una internet cuántica. El anuncio coincidió con la promesa firme de invertir 625 millones de dólares en el proyecto en un principio.

"Un equipo de físicos liderados por la Universidad de Harvard (Estados Unidos) ha logrado entrelazar dos nodos de memoria cuántica separados por 35 kilómetros usando como enlace fibra óptica existente en el área de Boston. Es la distancia más larga conseguida hasta la fecha. Según los autores, que publican los resultados en la revista Nature, demostrar que los nodos de una red cuántica pueden entrelazarse en el entorno real de una zona urbana muy transitada es un paso importante hacia la creación de redes prácticas entre ordenadores cuánticos" (Ramírez C. M., 2024).

Es importante recalcar que ese logro es importante debido a las siguientes razones: Primero, porque es la distancia más larga que se ha logrado para conectar nodos cuánticos en un ambiente urbano real; segundo, porque es un ejemplo de cómo las redes cuánticas se pueden construir utilizando el equipamiento de fibra óptica actualmente existente; y finalmente por destacar los retos siendo afectado por la distancia y los niveles de ruido en entornos muy concurrido por lo que lo convierte en una senda importante hacia redes cuánticas prácticas.

Además, empresas como IBM y Google están adentrándose en la computación cuántica con visión a largo plazo de integrarla en redes cuánticas. IBM ha estado desarrollando el sistema "IBM Quantum Network", que permite a los investigadores acceder a ordenadores cuánticos y también a plataformas para experimentar con la transmisión de información cuántica (Kjaergaard *et al*., 2020). La colaboración entre distintos laboratorios y empresas apunta a una creación más efectiva y rápida del marco necesario para el internet cuántico.

Caso de Europa: los europeos no se quedan atrás en la carrera por desarrollar un internet cuántico. La Unión Europea ha establecido el proyecto Quantum Internet alliance, que busca desarrollar una infraestructura cuántica en red. Este esfuerzo es respaldado por una combinación de laboratorios académicos y empresas. Uno de los líderes en este campo es la Universidad de Delft en los Países Bajos, donde se están llevando a cabo experimentos sobre

la creación de redes cuánticas que puedan conectar dispositivos cuánticos a través de telecomunicaciones convencionales (Van Loock *et al*., 2019).

Francia, por su parte, ha destacado en la creación de protocolos de encriptación cuántica. La realización de redes cuánticas de largo alcance ha sido un área clave de investigación, con planes para conectar múltiples ciudades a través de redes de fibra óptica y realizar pruebas de comunicación cuántica interurbana (Bacco *et al*., 2020).

3.5.Similitudes y diferencias entre el Internet clásico e Internet cuántico

De acuerdo a lo expuesto anteriormente, señalaremos las similitudes y diferencias entre Internet clásica vs. Internet cuántico.

Tabla 2 Comparativo de Internet clásico e Internet cuántico

Características	Internet clásico	Internet cuántico
Tipo de tecnología	Utiliza ondas de radio y cables de fibra óptica para transmitir datos.	Transmite los datos de manera más eficiente utilizando principios de la física cuántica.
Velocidad de transmisión	Velocidades típicas de hasta varios gigabits por segundo.	Potencialmente velocidades mucho más rápidas, incluso superando la velocidad de la luz.
Seguridad	Utiliza protocolos de seguridad estándar como RSA, SSL y VPN.	Utiliza la criptografía cuántica protege completamente la transmisión de datos.
Capacidad de procesamiento	Depende de la capacidad de los servidores y la infraestructura de red.	Potencialmente tiene una capacidad de procesamiento mucho mayor debido a la computación cuántica. (Gisin *et al*., 2002)
Conectividad	Dependiente de la infraestructura de red actual y puede haber problemas de congestión.	Ofrece una conectividad más estable y rápida, reduciendo la posibilidad de congestión en la red (Scarani *et al*., 2009).

Fuente: Elaboración propia.

3.6.Implicancias en la seguridad

3.6.1. El internet clásico en protección de la información

La computación favorece significativamente seguridad de datos como los siguientes mecanismos, el cual es de gran interés:

A. Criptografía:

Debemos recalcar que los algoritmos criptográficos clásicos se utilizan para resguardar los siguientes puntos, la garantía de integridad, autenticidad y confidencialidad de la información del usuario.

A continuación, pasamos a ver algunos ejemplos de algoritmos criptográficos clásicos los cuales son:

- Cifrado simétrico: Tal como señala Alcaraz y otros (2006) es estándar de cifrado avanzado conocida por sus siglas como AES, que funciona con tamaños de bloque fijos de 128 bits con claves que consiguen tener una extensión de 128, 192 o 256 bits. Esta flexibilidad permite un equilibrio entre velocidad y seguridad, en función de las necesidades; Data Encryption Standard o DES el cual su particularidad es que maneja una clave de 56 bits, a diferencia del AES, lo que se convierte en una mejor y seguridad (Medina Velandia, 2017); y por ultimo tenemos a Blowfish el cual tiene la particularidad de cifrar los datos en bloques de 64 bits con una clave cuya longitud varía hasta un 448 bits (Palacios & Delgado, 2006).
- Cifrado asimétrico: RSA, DSA, Elliptic Curve Cryptography (ECC).
- Funciones hash: SHA-256, SHA-3 y MD5.

La seguridad de estos algoritmos se fundamenta en el problema para solucionar problemas matemáticos complejos, como por ejemplo la descomposición en factores de números enteros realmente grandes o incluso la respuesta de logaritmos de tipo discretos

Tabla 3 Tipos de Cifrado simétrico

	DES	3DES	Blowfish	AES
Longitud de la clave	56 bits	112 or 168 bits	448 bits	128, 192, or 256 bits
Tamaño del bloque	64 bits	64 bits	64 bits	128 bits
Desarrollado en	1975	1978	1993	2000
Velocidad	Lento	Lento	Rápido	Rápido
Seguridad	No es lo suficientemente seguro	No es lo suficientemente seguro	Suficientemente seguro	Excelente seguridad
Estructura	Fiestel	Fiestel	Fiestel	Permutación por sustitución
Tiempo necesario para comprobar todas las claves posibles a 50 mil millones de claves por segundo	400 days	800 days	~3200 days	5×10^{21} days

Fuente: Ariel Shiftan, 2023, elaboración propia.

En la tabla 3 podemos ver que, si bien Blowfish es una de las buenas alternativas, su tamaño de bloque no es suficiente como AES. Consideramos a AES como el sucesor de DES como algoritmo de cifrado de clave simétrica para organizaciones. Acepta diferentes tamaños de clave, 128, 192 o 256 bits. Es eficiente tanto en software como en hardware. Además, podemos comprobar la eficacia de AES si analizamos el tiempo necesario para comprobar todas las claves posibles, a 50 mil millones de claves por segundo. Sus resultados son mucho mejores que los de otros algoritmos de cifrado, incluso si utiliza un tamaño de clave de 128 bits.

Tabla 4 Comparación de claves ECC y RSA

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Fuente: Ayoub, A., Najat, R., & Abouchabaka, J. (2018). An Overview on security schemes based on elliptic curve for Cloud-IoT. Elaboración propia.

En relación con el cifrado asimétrico, resaltan las claves RSA que tienen el tamaño recomendado, van aumentando para mantener una fuerza de cifrado suficiente, de 1024 bits a 2048 bits. Una alternativa a las claves RSA son las claves ECC. Estos dos tipos de claves maestras comparten la misma propiedad importante de ser algoritmos asimétricos (una clave para cifrar y una clave para descifrar). Sin embargo, ECC puede ofrecer el mismo nivel de potencia de cifrado para claves mucho más cortas, lo que proporciona una mejor seguridad al tiempo que reduce los requisitos informáticos (Ayoub y otros, 2018). Finalmente, en la tabla 4 podemos resaltar que la diferencia clave entre ECC y RSA es el tamaño de la clave en comparación con la fuerza del cifrado.

B. Autenticación:

Los mecanismos de autenticación clásicos son usados para poder comprobar la autenticidad de los datos proporcionada por los usuarios y las entidades. Algunos ejemplos de mecanismos de autenticación clásicos son:

- Contraseñas: Un método simple pero común de autenticación.
- Factores de autenticación múltiples (MFA): Combinan diferentes factores, como contraseñas, códigos de un solo uso (OTP) o datos biométricos, para mejorar la seguridad.
- Certificados digitales: Manejan criptografía de clave tipo pública para verificar la identidad de sitios web y principalmente de los usuarios.

C. Control de acceso:

Los sistemas tradicionales que corresponden al control de acceso restringen el acceso a recursos confidenciales en otras palabras, se basan en listas de control de acceso o también conocidas como ACL por sus siglas en inglés, y que es responsable de determinar qué usuarios o organizaciones tienen autorización para tener acceso a qué tipo de recursos.

D. La detección de intrusiones:

Los sistemas clásicos que se encargan de detección de las intrusiones se utilizan para identificar y prevenir actividades no autorizadas en redes y sistemas informáticos. Es decir, utilizan una variedad de técnicas, como el análisis de registros, la detección de anomalías y la firma de intrusiones, para identificar actividades sospechosas.

E. Protección de datos:

Las técnicas de protección de datos clásicas según Granados (2006) se utilizan para salvaguardar los datos a nivel de integridad, confidencialidad y la disponibilidad de los datos. Es por ello que a continuación ejemplificaremos algunas de las técnicas de protección de datos clásicas y estas son:

- **Cifrado:** que consiste en convertir los datos en un formato ilegible para que exclusivamente los usuarios permitidos puedan usarlos.
- **Control del acceso**: Restringir el acceso a los datos solo a los usuarios y entidades que los necesitan.
- **Crear copias de seguridad**: hace referencia al proceso de hacer 'backups' de los datos para garantizar su disponibilidad que puedan restaurarse en caso de que se pierdan o se corrompan.

Briceño (2021) ha afirmado respecto a ciberseguridad que:

La seguridad de la información se ha vuelto crucial en diversos aspectos de nuestra sociedad interconectada, principalmente por la amplia adopción de tecnologías de información y comunicación. Diariamente, utilizamos computadoras para trabajar, estudiar en línea, realizar compras y acceder a correos electrónicos en diferentes ubicaciones. Además, llevamos nuestros teléfonos inteligentes a todas partes, utilizándolos para verificar saldos bancarios, monitorear actividad física y gestionar otros aspectos de nuestra vida cotidiana. (Briceño E. V., 2021, pp 9).

Otros como Gilberg, R., & Valli, C. (2017) indican que la proliferación de dispositivos conectados está transformando la seguridad de la información y la necesidad de asegurar estos sistemas, por lo que la estrategia de ciberseguridad se está convirtiendo en un aspecto crítico en la protección de nuestra sociedad interconectada. Es por ello por lo que, aunque la tecnología nos vuelve más eficientes y nos brinda la oportunidad de obtener acceso a un vasto conjunto de datos con un solo clic, no obstante, afronta muchos desafíos de seguridad.

Debido a la ciberdelincuencia y las repercusiones graves que podrían tener. Se debe resaltar que a causa de un riesgo de la configuración del sistema que facilita un ataque por parte de un intruso acceder al sistema de gestión de bases de datos (SGBD) la cual alberga información

de propiedad exclusiva puede describirse como información confidencial o información propietaria. Ambas expresiones son comunes en el contexto de la protección de datos y la seguridad de la información, nuestro administrador podría obtener pérdidas millones de dólares, juzgar procesamiento legal y afrontar ataques a su honorabilidad. Hoy en día, es más frecuente que pasados cinco, diez o veinte años, que los canales locales o internacionales transmitan información acerca de fraudes informáticas.

La ISO/IEC (2018) ofrece una "descripción general de los sistemas de gestión de seguridad de la información (SGSI). También proporciona términos y definiciones que se utilizan comúnmente en la familia de normas SGSI. Este documento es aplicable a organizaciones de todo tipo y tamaño" (ISO & IEC, 2018). Es decir, la ISO/IEC define la protección de los datos como actividades, excelentes estrategias y metodologías que protegen los datos y los sistemas de documentos del registro, uso, comunicación, acortamiento, transformación o demolición que no está permitida.

Según esta conceptualización, logramos preservar nuestra infraestructura tecnológica y datos cualquier persona que intente hacer un mal uso de ellos. Por otro lado, en un sentido general, la seguridad se refiere a la protección de nuestros activos. Esto puede significar protegerlos de cortes de energía, desastres naturales, condiciones ambientales desfavorables, robo o vandalismo u otros estados indeseables.

Podemos pensar en objetos tangibles que podemos desear preservar, a modo de esos que tienen valor intrínseco (como los almacenes de oro de un banco) o las que presentan importancia para nuestra empresa. Además, lograremos tener componentes más fluidos, como programas, aplicaciones fuente o datos. Es posible que nos demos cuenta como nuestros recursos lógicos sean poco importantes, si no aún más, nuestros recursos hadrware, esto incluye todos los dispositivos tangibles, como servidores, computadoras, routers, y otros componentes de infraestructura tecnológica en el contexto tecnológico hoy en día lo sean.

Los impactos de la protección que decidimos ejecutar además ameritamos considerar en nuestras iniciativas por proteger nuestros recursos. Aunque lograríamos argumentar que un sistema en tal situación sería capaz ser correctamente seguro, es indudable que no es provechoso ni eficiente. Aunque incrementar la seguridad suele causar una disminución de los rendimientos, es necesario lograr un balance (Briceño E. V., 2021).

Además de lo anterior mencionado, al cuidar un contenido, sistema o ambiente, hemos de evaluar a través de qué el grado de seguridad se conecta con el valor del contenido que se encuentra protegiendo. Intentamos utilizar grados elevadísimos de seguridad a cualquiera los recursos de los que nos encontramos obligados si situamos establecidos en ajustarnos a la reducción de la efectividad. Pese a que logremos construir una estructura de miles de o incluso millones de dólares, aquel ambiente en el que diseñamos y creamos grados altos de protección, debemos de tener en conocimiento el gasto de substituir nuestros activos si los logramos perder y protegernos de que su valor sea protegido a un costo razonable. Es decir, nunca debemos dejar que el gasto de la protección que realizamos sea más elevado que el importe de lo que asegura.

Si bien los ataques a la protección de la información tienen principalmente que ver con actos de manera inconsciente o errores humanos, o hasta incluso desastres naturales. La realización de un ataque puede permitir el acceso, la transformación o la desaparición de información que no está permitida; el procesamiento de un sistema o la interrupción de algún servicio; el asalto o ataque a los dispositivos y recursos que se encargan de guardar los datos. En relación a lo anterior, mencionaremos las amenazas más comunes respecto a vulnerar la seguridad de la información de datos.

- *Spywre* (Programas espías): Código peligroso cuya misión principal es recaudar datos sobre las operaciones de un administrador en un PC, como autorizar el desarrollo sin permiso de aplicaciones emergentes según sus hábitos de navegación es de publicidad comercial o robar información personal, además de los claves de tarjetas de pago. Hay planes para usarlos para regular el uso de aplicaciones ilegal. Según algunos datos, aproximadamente el 91% de los equipos tienen spyware instalado, y según un informe de EarthLink después de una evaluación de aproximadamente alrededor de un millón de computadoras presentes en la red, la cantidad de los programas "spyware" que poseía cada equipo llegaba a 28, una cantidad alarmante.
- *Troyanos, malware y gusanos*: Estos vienen a ser aplicaciones de código peligroso los cuales se almacenan en dispositivos de diferentes formas para otorgar a un pirata el ataque no otorgado o el dominio remoto de los equipos. Además, el virus tiene de propósito fundamental destruir información y ser dañino para la máquina o generar el derroche incontrolado de recursos para llegar a bloquear o no permitir acceder a distintos servicios que el usuario requiere.

Es importante recalcar que el vector que propaga estos códigos suele ser otro programa o archivo es decir puede ser un programa ejecutable que pase desapercibido, una imagen que nos parezca conocida, un video, reproducciones flash, incluso alguna música que nos guste y muchos otros; por otro lado, es muy común que los virus se repliquen automáticamente una vez que se instalan en el sistema del equipo.

Según las estadísticas, se generan cientos de estos programas cada mes, cuyo principal objetivo es el robo financiero, poniendo en riesgo más que la destrucción de archivos la información confidencial y el dinero de las personas y las organizaciones. Los criptovirus son la clase de virus más popular en la actualidad, una vez que se instalan, cifran la información en el disco del equipo o algunos archivos contenidos en él (Tarazona, 2007).

•Phishing: al respecto sabemos que es un tipo de ataque que tiene como propósito obtener información confidencial de un determinado usuario, principalmente financiera, aprovechando la confianza del usuario en los servicios tecnológicos, su escasez de conocimiento sobre cómo funcionan y, en ciertos escenarios, proporcionando servicios con técnicas de seguridad inadecuadas.

Cabe resaltar que actualmente, los hechos relacionados con el phishing son enormemente avanzados y se apoyan en noticias electrónicos y sitios web falsos como a su vez funcionan como los primeros sitios web.

• Spam: Recibir datos no exigidos, en su mayoría enviados por e-mail electrónico, que tienen como objetivo difundir una gran cantidad de propaganda o mensajes mercantiles están presentado casos en los que los envíos se han enviado a los sistemas de mensajes de texto de los celulares o a los sistemas de fax. Algunos autores señalan que “Se estimó que entre el 60 y el 70 % de los correos electrónicos eran “spam” con contenido comercial o pornográfico en 2006” (Tarazona, 2007,pp 139).

•Botnets: respecto a ello sabemos que son dispositivos corrompidas y ejecutadas de manera remota, las cuales actúan como “maquinas infectadas” y se conectan por medio de redes descentralizadas de computadoras llamadas bot. Estos robots transmiten numerosos correos electrónicos de tipo 'spam' o que contienen código malicioso con el propósito de vulnerar otros sistemas.

•Trashing o dumpster diving: Los sistemas de contenidos confidencial no están relacionados de manera directa al método de atención como datos temporales utilizado por ciberdelincuentes. Para lograrlo, buscan en la basura de las personas y empresas para recopilar datos personales, contraseñas y otra información personal que puede ser utilizada de manera fraudulenta, y luego los emplean para crear una cuenta de usuario que contenga la información pública y privada de la víctima para apropiarse de sus credenciales y obtener los accesos para toda su data personal.

Finalmente debemos saber que, para prevenir convertirse en la causa de ataques a otras redes o tecnologías avanzadas, las instituciones deberían examinar los ordenadores de sus redes de datos para identificar indicios sobre estas infecciones relacionados siguiendo este modelo (Tarazona, 2007). Para ello, los últimos usuarios, las empresas que ofrecen acceso a la red y quienes prestan servicios como se denominan "cibercafé" y tiendas deben colaborar y contribuir constantemente a este objetivo.

3.6.2. El internet cuántico y sus implicancias en la seguridad de la información.

El internet cuántico representa un avance revolucionario en las tecnologías de comunicación y en la seguridad de la información. Basado en principios de la mecánica cuántica, permite la transmisión de información a través de qubits, que a su vez pueden asentar las bases de un sistema de comunicación que es básicamente más seguro que las tecnologías actuales.

Una de las implicaciones más significativas del internet cuántico es su capacidad para implementar la criptografía cuántica. A través de la Distribución de Claves Cuánticas (QKD), es posible generar y compartir claves criptográficas de manera que cualquier intento de interceptación sea detectable. Por ejemplo, el protocolo BB84, propuesto por Bennett y Brassard en 1984, establece las bases para la transmisión de claves seguras utilizando propiedades cuánticas. La QKD se basa en el principio de que medir un qubit implica un cambio en su estado, lo que permite a las partes involucradas identificar si ha habido un espionaje (Bennett & Brassard, 1984). Esto garantiza un nivel de seguridad que las técnicas criptográficas clásicas no pueden ofrecer.

Además de la criptografía cuántica, el entrelazamiento cuántico proporciona un nuevo paradigma para la seguridad en la comunicación. En este contexto, si dos qubits están entrelazados, cualquier cambio en uno afectará instantáneamente al otro, sin importar la distancia que los separe. Este fenómeno permite el desarrollo de protocolos de comunicación

que son robustos ante intentos de interferencia y proporcionan una confianza sin precedentes en la integridad de los datos transmitidos (Nielsen & Chuang, 2010).

Respecto a la autenticación mejorada, debemos saber que los protocolos cuánticos también permiten sistemas de autenticación más robustos. Por ejemplo, la verificación de identidad se simplifica al utilizar estados cuánticos, aumentando la seguridad de las transacciones en línea y otros servicios críticos (Mattle *et al*., 1996).

En cuanto los desafíos tecnológicos y de escalabilidad, la tecnología cuántica está en una fase de desarrollo y enfrenta desafíos como la creación de qubits estables y la superación de la pérdida de señal en largas distancias. Estos problemas técnicos podrían dar lugar a períodos de vulnerabilidad hasta que se aborden adecuadamente (Ladd *et al*., 2010).

A. Corrección de errores

Uno de las fundamentales competencias del es la reparación de defectos, internet cuántico. Debido a la naturaleza inestable de los qubits, es común cometer errores durante el cálculo, lo que puede resultar en resultados incorrectos. En contraste, los errores en la informática convencional se pueden detectar y corregir fácilmente. A pesar de los avances en la corrección de errores cuánticos, la disciplina sigue enfrentando importantes desafíos.

B. Eficiencia Energética

El internet cuántico es menos eficiente energéticamente que la computación tradicional porque necesita mucha energía para funcionar. Esto se debe a que el mantenimiento de las computadoras cuánticas requiere mucha energía, ya que requieren temperaturas extremadamente bajas para operar adecuadamente, lo que implica un alto consumo energético para su mantenimiento. Esta necesidad se debe a la conservación de la coherencia cuántica y la minimización de la interferencia térmica que pueda afectar el rendimiento de los qubits. (Devoret *et al*., 2004)

La corrección de errores y la eficiencia energética son algunos de los muchos desafíos que aún quedan por resolver para aprovechar plenamente el potencial del internet cuántico. Sin embargo, es probable que el internet cuántico sea cualquier vez más crucial en una enorme variedad de utilizaciones a medida que se sigan realizando avances en este campo.

3.7.Implicancias en la transmisión de la información

El internet cuántico se presenta como una innovadora evolución en la transmisión de información, aprovechando las propiedades únicas de la mecánica cuántica para mejorar la seguridad y la eficiencia en las comunicaciones. A medida que nuestra sociedad avanza hacia una mayor conectividad y dependencia de los datos, entender las implicancias del internet cuántico se vuelve esencial para el futuro de la ciberseguridad y las telecomunicaciones.

Una de las implicancias más significativas del internet cuántico es su capacidad para proporcionar una comunicación extremadamente segura. A diferencia de los sistemas de comunicación tradicionales, que pueden ser vulnerables a escuchas y ataques, el internet cuántico utiliza el principio de la superposición cuántica y el entrelazamiento. Estos principios garantizan que cualquier intento de interceptar, medir o copiar un estado cuántico implica una alteración del propio sistema, lo que permite a las partes comunicantes detectar inmediatamente cualquier intrusión (Bennett & Brassard, 1984). Este nivel de seguridad se traduce en la posibilidad de enviar información confidencial sin el riesgo de que sea interceptada, lo que es crucial en sectores como el bancario, la salud y la defensa.

Además de la seguridad, el internet cuántico tiene el potencial de aumentar significativamente la velocidad de transmisión de datos. Al utilizar qubits en lugar de bits, es posible procesar y transmitir información de una manera que no es factible con la computación clásica. Los qubits pueden existir en múltiples estados simultáneamente, lo que permite una mayor capacidad de procesamiento y una disminución en los tiempos de latencia. Investigaciones sugieren que, con el desarrollo de redes cuánticas, se podría lograr una comunicación a velocidades mucho mayores que las que actualmente ofrece la infraestructura convencional (Pirandola *et al*., 2017).

Otra implicancia importante es la mejora en la calidad de la comunicación y la reducción de errores en la transmisión de datos. La comunicación cuántica tiene la capacidad de corregir errores de manera más eficiente a través de la codificación cuántica, lo que puede resultar en una transmisión de información más fiable a largas distancias. Este avance puede ser especialmente relevante para el envío de información sensible, donde la integridad es fundamental.

Sin embargo, la implementación del internet cuántico enfrenta desafíos técnicos significativos. La creación de una infraestructura cuántica robusta implica superar dificultades en la generación, el mantenimiento y la transmisión de qubits. Esto requiere avances en

tecnología de fibra óptica y sistemas de red que puedan soportar las características únicas de las señales cuánticas. Además, se necesita un marco normativo adecuado para asegurar que las aplicaciones cuánticas sean seguras y efectivas (Kurochkin, 2020).

Finalmente, el internet cuántico representa un cambio de paradigma en la manera en que se transmitirá la información en el futuro. Su potencial para ofrecer comunicación segura y rápida tiene implicancias profundas en diversos sectores, desde la ciberseguridad hasta la protección de datos personales. No obstante, los retos tecnológicos, éticos y regulativos deben ser abordados para que el internet cuántico pueda integrarse de manera efectiva y segura en nuestra sociedad.

CONCLUSIONES

Esta tesis concluye que el internet cuántico es una posible evolución del internet clásico utilizando principios de la física cuántica y aunque hasta la actualidad se han logrado avances significativos en la transmisión de información cuántica a través de distancias cada vez mayores, el internet cuántico como tal aún no existe en su forma completa y funcional.

Por lo tanto, podemos concluir que a diferencia del internet clásico que se fundamentado en el razonamiento de que un componente únicamente podría ser una característica a la ocasión, o un 0 o un 1. En el internet cuántico estos ceros y unos se superponen simultáneamente. Esto le da a Internet cuántico una gran ventaja: reduce la vulnerabilidad de ser hackeado y sería mucho más rápido en la transmisión de información.

Podemos concluir que el internet cuántico es el resultado de décadas de investigación en múltiples disciplinas, con contribuciones clave de varios científicos y teóricos que han avanzado en comprensión y aplicación de los principios cuánticos en la informática y la comunicación.

Asimismo, podemos concluir que el internet cuántico tiene el potencial de superar al internet clásico en varios aspectos, especialmente en términos de velocidad y seguridad. Puede transmitir grandes volúmenes de datos a velocidades superiores a la del internet clasico y permite la coexistencia de datos cuánticos y clásicos sin interferencias. Sin embargo, el internet cuántico no es necesariamente mejor que el internet clásico en todas las aplicaciones y todavía se encuentra en desarrollo por lo que no está ampliamente disponible.

Finalmente, podemos concluir que el futuro del internet cuántico incluye desafíos como la construcción de redes cuánticas globales, computadoras cuánticas, mejorar la confiabilidad y eficacia de los sistemas cuánticos, y la integración con aplicaciones prácticas como la computación distribuida y la seguridad cibernética avanzada.

Bibliografía

Aaronson, S. (2013). Quantum computing since Democritus. *Cambridge University Press*, 56.

Aguado, D. G. (2022). Protocolos de criptografía asistida por QKD. Universidad Politécnica de Madrid.

Alcaraz, C., Roman, R., & López, J. (2006). Análisis de primitivas criptográficas para redes de sensores.

Aristizabal, V. H. (2017). Introducción a la Tecnología de Fibras Ópticas y Análisis Numérico de la Propagación de la Luz en Fibras Micro-Estructuradas. *Tecno Lógicas*(19), 141-165.

Ayoub, A., Najat, R., & Abouchabaka, J. (2018). An Overview on security schemes based on elliptic. *Journal Of Advances In Natural Sciences, 5*(1), 352-361.

Bell, J. (1964). On the Einstein Podolsky Rosen paradox. *Physics, 1*, 195-200.

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*(560), 175-179. https://doi.org/10.1016/j.tcs.2011.08.039

Berners-Lee, T. (1999). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web.* Harper San Francisco.

Bohman, J. (2010). On the Internet. *Routledge*.

Briceño, E. V. (2021). Seguridad de la información. 3Ciencias.

Caleffi, M. (2021). Advances in quantum networks: from the fundamentals to practical applications. *Applied Sciences, 11*(15). https://doi.org/6827

Cerf, V., & Kahn, R. E. (1974). A Protocol for Packet Network Intercommunication. *IEEE Transactions on Communications*.

Claramunt Carriles, S. (mayo de 2022). Computación cuántica en la seguridad informática. 30-31. https://doi.org/http://hdl.handle.net/10045/124691

Devoret, M. H., Wallraff, A., & Martinis, J. M. (2004). Superconducting Qubits: A Short Review. *Science*. https://doi.org/arXiv:cond-mat/0411174

Fang, K., Zhao, J., Li, X., Li, Y., & Duan, R. (2023). Quantum NETwork: from theory to practice. *Science China Information Sciences, 66*(8). https://doi.org/10.1007/s11432-023-3773-4

Franchi, M. R. (2012). Algortimos de encriptación de clave asimétrica. *Tesis Doctoral*. Universidad Nacional de La Plata.

Friedman, T. L. (2005). *The World is Flat: A Brief History of the Twenty-First Century.* Farrar, Straus and Girou.

Fuentes Herrera, A. J. (2017). El control interno aplicable a la seguridad de la información para sistemas contables computarizados según ISO 27001 en empresas comercializadoras de productos de telecomunicación del área metropolitana de San Salvador. Universidad de El Salvador.

Gilberg, R., & & Valli, C. (2017). Cybersecurity: The Role of the National Cybersecurity Strategy. *Computer Law & Security Review, 33*(4), 491-508.

Gisin, N., & Fasel, S. (1998). Quantum Communication with Photons. *Physical Review Letters , 98*. https://doi.org/10.1103/PhysRevLett.98.020503

Gisin, N., Ribordy, G., Tittel, W., Zbinden, &., & H. (2002). Quantum Cryptography. *Reviews of Modern Physics, 74*(1), 145-198. https://doi.org/https://doi.org/10.1103/RevModPhys.74.145

Gordon, D. (1998). The Internet's Impact on Society and Economy. *Communications of the ACM, 41*(11), 15.

Granados Paredes, G. (2006). Introducción a la criptografía.

HUB, I. (14 de agosto de 2022). *INNOVATION HUB*. https://www.aecoc.es/innovation-hub-noticias/redes-de-comunicacion-ultra-seguras-la-base-de-la-red-de-internet-cuantica/

ISO, & IEC. (2018). *SO/IEC - International Organization for Standardization and International Electrotechnical Commission*. https://www.iso.org

Iván García-Cobo, Á. M. (2022). GESTIÓN INTELIGENTE DE RED CUÁNTICA. *Proceedings of the IV Workshop on Disruptive Information and Communication Technologies for Innovation and Digital Transformation*, 105-116. https://doi.org/https://doi.org/10.14201/0AQ0315105116

Kjaergaard, M., Schwartz, M. E., Braumüller, J., Krantz, P., Wang, J. I.-J., Gustavsson, S., & Oliver, W. D. (2020). Superconducting Qubits: Current State of Play. *Annual Review of Condensed Matter Physics, 11*, 369-395. https://doi.org/https://doi.org/10.1146/annurev-conmatphys-031119-050605

Kurochkin, Y. (2020). Development of quantum communications. *Quantum Electronics, 50*(5), 425-425. https://doi.org/10.1070/QEL17353

Leiner, B. M. (2009). A brief history of the Internet. *ACM SIGCOMM computer communication review, 39*(5), 22-31.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review, 39*(5), 22-26. https://doi.org/https://doi.org/10.1145/1629607.162961

Liao, S.-K. e. (2017). Satellite-Relayed Intercontinental Quantum Network. *Physical Review Letters, 119*(6). https://doi.org/10.1103/PhysRevLett.119.060501.

Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., ... (2017). Satellite-to-ground quantum key distribution. *Nature, 549*(7670), 43–47. https://doi.org/10.1038/nature23655

Licklider, J. C. (2002). *Historia de Internet.* Boston, Estados Unidos.

Liu, J.-L., Luo, X.-Y., Yu, Y., Wang, C.-Y., Wang, B., Hu, Y., . . . Yan, Z. (2024). Creation of memory–memory entanglement in a metropolitan quantum network. *Nature, 629*, 579–585. https://doi.org/https://doi.org/10.1038/s41586-024-07308-0

López, E. (2017). El entrelazamiento cuantico. Mexico.

Matsuo, S. e. (2020). Quantum Internet: A new paradigm for distributed quantum computation. *Journal of Quantum Information Science, 10*(2), 50-67.

Medina Velandia, L. N. (2017). Criptografía y mecanismos de seguridad.

Nebreda Rodrigo, I. (2013). El origen de Internet. El camino hacia la red de redes. Universidad Politécnica de Madrid. https://oa.upm.es/22577/1/PFC_IVAN_NEBREDA_RODRIGO.pd

Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge: Cambridge University Pres.

Noiri, A. T. (2022). Fast universal quantum gate above the fault-tolerance threshold in silicon. *Nature, 601*, 338–342. https://doi.org/https://doi.org/10.1038/s41586-021-04182-y

O'Reilly, T. (2007). What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *University Library of Munich, Germany, MPRA Paper, 65*.

Ortiz Rojas, H. (2007). Fundamentos de criptografía cuántica. *Tesis de Licenciatura*. Universidad EAFIT.

Palacios, R., & Delgado, V. (2006). Introducción a la Criptografía: tipos de algoritmos. anales de mecánica y electricidad.

Pastor Collado, J., & Elias Vila, E. (2017). *Internet. Funcionamiento, aplicaciones y seguridad.* Universitat Oberta de Catalunya.

Pirandola, Bardhan, S. a., Gehring, B. R., Weedbrook, T. a., Lloyd, C. a., & S. (2018). Advances in photonic quantum sensing. *Nature Photonics, 12*(12), 724–733. https://doi.org/10.1038/s41566-018-0301-6

Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A., & Braunstein, S. (2015). Advances in Quantum Teleportation. *Nature Photonics, 9*. https://doi.org/10.1038/nphoton.2015.154

Primera, R. (2004). Computadores cuánticos paradoja de la superposición. *3, 1*, 59-69. Télématique.

Qubits meet materials science. (2021). *Nat Rev Mater, 6*, 869. https://doi.org/https://doi.org/10.1038/s41578-021-00378-w

Ramírez, H. D., Contreras, R., Espinoza, N. B., & Huerta, Y. (2021). Fundamentos del Álgebra Lineal en la Computación Cuántica. *Gustavo Trinidad Rubín Linares*, 66.

Ruiz, C. (2021). Sobre la Computacion Cuántica. *UNED*, 26-27.

Sacristán, E. (2017). Un avance hacia las comunicaciones cuánticas. Ciencia contada en Español.

Salinas Anaya, Y. D., Galván Rodríguez, D. G., Guzmán Prince, I., & Orrante Sakanassi, J. A. (2022). El impacto del internet de todas las cosas (IoT) en la vida cotidiana. *6, 2*, 1369-1378. Ciencia Latina Revista Científica Multidisciplinar.

Scarani, V., Bechmann-Pasquinucci, H., Briegel, H.-J. D., & Wehner, S. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics, 81*(3), 1301-1350. https://doi.org/https://doi.org/10.1103/RevModPhys.81.1301

Schott. (agosto de 14 de 2022). *We make things visible*. http://www.us.schott.com/fiberoptics/englishlindex.html?c=aL

Shankar, R. (1994). *Principles of quantum mechanics* (2 ed.). Quantum theory. https://doi.org/0-306-44790-8

Sharma, P. A. (2021). Distribución de claves cuánticas redes ópticas seguras: una encuesta. *IEEE Open Journal de la Sociedad de Comunicaciones*.

Shiftan, A. (2023). *Piiano.com*. https://www.piiano.com/blog/column-level-encryption

shutterstock. (16 de diciembre de 2018). *shutterstock*. https://www.shutterstock.com/es/image-vector/qubit-vs-bit-states-classical-compare-1259122546

Sillanpää, M., & HakonenPertti J. Hakonen, P. (2015). Conexiones para una red cuántica. *Investigación y Ciencia*.

Sputnik, M. (23 de diciembre de 2020). Un nuevo descubrimiento de la NASA nos acerca a la Internet cuántica. https://mundo.sputniknews.com/20201223/un-nuevo-descubrimiento-de-la-nasa-nos-acerca-a-la-internet-cuantica-1093927700.html

Tapscott, D., & Williams, A. (2006). *Wikinomics: How Mass Collaboration Changes Everything.* Portfolio.

Tarazona, C. H. (2007). Amenazas informáticas y seguridad de la información. *Derecho penal y criminología, 28*, 137.

Wu, Y. B. (2021). Strong Quantum Computational Advantage Using a Superconducting Quantum Processor. *Physical review letters, 127*(18). https://doi.org/180501

Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., ... (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science, 356*, 1140-1144. https://doi.org/10.1126/science.aan3211

Zapata Godoy, J., Brenes Pacheco, E., & Rodríguez Bravo, C. (2021). ¿Es la computación cuántica el fin de la computación clásica? . *LOGOS, 2*(1), 68-76.

Zittrain, J. (2009). The Future of the Internet and How to Stop It. *Yale University Press*.