UNIVERSIDAD SIMÓN BOLÍVAR
Vicerrectorado Académico

1 .Departamento: Física

2. Asignatura: **Información y Comunicación Cuántica Avanzada III**

3. Código de la asignatura: FS-7451

No. de unidades-créditos: 4

No. de horas semanales: Teoría 4 Práctica 2 Laboratorio 0

4. **Fecha de entrada en vigencia de este programa:** Enero 2017

5. Requisitos: Información y Comunicación Cuántica Avanzada II (FS-7450)

6. OBJETIVO **GENERAL:** Esta asignatura, tiene como objetivo principal, el capacitar a los estudiantes en el estudio de los grafos cuánticos y sus aplicaciones, tanto en sistemas de comunicación cuántica, como en el desarrollo de redes cuánticas.

7. (Opcional) **OBJETIVOS ESPECÍFICOS:** El estudiante tendrá competencias para:

.

1. Dominar los conceptos básicos asociados a grafos cuánticos, así como sus aplicaciones en el desarrollo de circuitos cuánticos, y en la teoría de corrección de errores en computación cuántica.
2. Entender la relación existente entre los estados estabilizadores y los grupos de Clifford.
3. Entender y desarrollar protocolos de comunicación con estados grafos, estados estabilizadores y estados clúster.

4.- Entender los fundamentos cuánticos básicos de las arquitecturas de redes cuánticas, sus arquitecturas y distribución de llaves cuánticas.

5.- Dominar los elementos conceptuales y metodológicos básicos para la implementación experimental en áreas de investigación básica y la formulación de proyectos sencillos de comunicación cuántica segura, en procesos de transferencia de información sensible en el área empresarial y de investigación básica.

8. CONTENIDOS:

1.- GRAFOS CUANTICOS:

1.a) Definiciones de grafos cuánticos. Estados Clusters, estados estabilizadores y el modelo de Ising. Grupo de Clifford. Estados grafos y formalismo estabilizador. Evolución de un estado grafo a través de su estabilizador. Función de Lovász de un grafo.

1.b) Grafos para compuertas de un solo qubit. Grafos para compuertas de dos qubits. Grafos QCNOT. Grafos entrelazados: clases de equivalencia, complementación local, criterios de clasificación. Conjunto compacto de invariantes para estados grafos bajo operaciones locales estocásticas asistidas por comunicación clásica (SLOCC). Invariantes de Van den Nest, Dehaene y De Moor.

2.- PROTOCOLOS CON GRAFOS CUANTICOS: Códigos de corrección cuántica usando estados grados de qudits. Protocolos de Teleportación y Codificación Densa usando grafos cuánticos. Códigos criptográficos.

3.- GRAFOS CUANTICOS Y FUNDAMENTOS DE LA MECANICA CUANTICA: Paradoja de EPR, Teoría de las variables ocultas, Desiqualdades de Bell. Demostraciones "all-versus nothing (AVN)" del teorema de Bell. Desigualdad de Clauser-Horne-Shimony-Holt (CHSH). Teorema de Gleason. Teorema de Kochen-Specker. Desigualdad de Klyanchko-Can-Binicoglu-Shumovsky (KCBS). Medida condicional en modelos no contextuales de variables ocultas. Demostraciones AVN bipartitas y m partitas usando estados grafos. Estudio las violaciones a las relaciones de Localidad y Contextualidad con grafos con múltiples fotones. Relaciones de monogamia para localidad y Contextualidad con estados grafos.

4.- ARQUITECTURA DE UNA RED CUÁNTICA: Componentes y dispositivos físicos de un canal criptográfico, codificación. Análisis de QKD en sistemas de fibras ópticas y en la transmisión de información en espacios libres a largas distancias. Seguridad incondicional en las redes inalámbricas usando QKD. Estrategias de conexión. Intercambio de una clave. Concordancia de llaves cuánticas a dos partes. Destilación de la clave. Estimación de la información del intruso. Autenticación. Cifrado y distribución de llaves. Grafos cuánticos en redes cuánticas.

5.- REDES DE DISTRIBUCIÓN CUÁNTICA DE LLAVES: Redes punto a punto. Redes públicas o privadas. Anillo de distribución. Configuración en estrella. Canal compartido. Topología de llaves cuánticas a nodos. Niveles de una red cuántica. Autenticación y certificación. Estrategias de ataques. Vulnerabilidad. Redes cuánticas y de interconexión. Computación distribuida y Comunicación Digital. Entrelazamientos conjuntos como marcos de referencia. Selección de rutas para redes de repetidores cuánticos. Afinando las limitaciones clave. Repetidores Cuánticos: enrutamiento, gestión y multiplicación de recursos, repetidoras cuánticas a grandes distancias, clasificación de los ataques a repetidoras cuánticas. Internet Cuántico.

6.-SISTEMAS DE CRIPTOGRAFÍA CUÁNTICA EN LA EMPRESA: Necesidades empresariales de seguridad cuántica en la comunicación. Tipos de empresas existentes: Clasificación, productos que ofertan, costos, servicios en el mercado internacional en el área de comunicación segura. Requisitos mínimos para la formulación de un proyecto. Estudios de costos/beneficios. Criterios para formular y ejecutar un proyecto de criptografía cuántica eficiente. Aplicaciones experimentales de las redes cuánticas en investigación básica, y su importancia para el desarrollo de las nuevas tecnologías.

9. **ESTRATEGIAS METODOLÓGICAS, DIDACTICAS O DE DESARROLLO DE LA ASIGNATURA.**

Se recomiendan las siguientes:

1. Clases magistrales
2. Sesiones de Ejercicios y/o Problemas
3. Talleres y seminarios
4. Investigaciones
5. Presentaciones
6. Simulaciones computarizadas

10. ESTRATEGIAS DE EVALUACIÓN.

Se recomiendan las siguientes:

1. Pruebas escritas y/o verbales
2. Informes de simulaciones de protocolos y su transmisión por redes cuánticas
3. Ejercicios, tareas y/o asignaciones para realizar fuera del aula.
4. Búsqueda de publicaciones científicas e ingenieriles, relevantes y novedosas en el área de la criptografía cuántica, así como una explicación completa y detallada, del contenido de las mismas, en exposiciones orales y/o escritas.
5. Investigación de problemas específicos en investigación básica, así como la formulación de propuestas para resolverlos usando los conocimientos aprendidos en el curso.

11. FUENTES DE INFORMACIÓN:

1.- Gregory Berkolaiko, Peter Kuchment, " Introduction to Quantum Graphs", (Mathematical Surveys and Monographs) Volume 186. American Matematical Society. Applied Mathematics. (2013)

2.- Sandor Imre and Laszlo Gyongyosi "ADVANCED QUANTUM COMMUNICATIONS: An Engineering Approach", John Wiley and Sons, INC., Publication, (2013)

3.- Van Meter, "Quantum Networking", Jhon Wiley and Sons, (2014)

4.- M. A. Nielsen y I. L. Chuang, Quantum computation and quantum information, Cambridge University Press, (2010)

5.- M. A. Nielsen y I. L. Chuang, "Quantum computation and quantum information", Cambridge University Press, (2010).

6.- Mikio Nakahara and Tetsuo Ohmi, "Quantum Computing, from Linear Algebra to Physical Realizations". CRC Express. (2008)

7.- R. Carlson, S. A. Fulling, and P. K. Gregory Berkolaiko, "Quantum Graphs and Their Applications", (Contemporary Mathematics) (2006)

8.- Peter Kuchment, Quantum graphs: an introduction and a brief survey, Proc. Symp. Pure. Math., AMS (2008), pp.291 – 314

9.- Sandor Imre and Laszlo Gyongyosi "ADVANCED QUANTUM COMMUNICATIONS: An Engineering Approach", John Wiley and Sons, INC., Publication, (2013)

10- Asher_Peres, "Quantum Theory Concepts and Methods", Kluwer Academic Publishers. (2002)