UNIVERSIDAD SIMÓN BOLÍVAR
Vicerrectorado Académico

1 .Departamento: *Física*

2. Asignatura: COMUNICACION CUANTICA

3. Código de la asignatura:

No. de unidades-créditos: 3

No. de horas semanales: Teoría 3 Práctica 2 Laboratorio 0

4. Fecha de entrada en vigencia de este programa:

5. Requisitos: *FS*-5445 INFORMACION CUANTICA BASICA

6. OBJETIVO GENERAL: *Formar a los estudiantes con los conceptos y las herramientas fundamentales de uso en las comunicaciones cuánticas, y en el entendimiento de los procesos de transmisión de información por canales cuánticos, haciendo énfasis en la criptografía cuántica y en la distribución de llaves cuánticas.*

7. *(Opcional)* OBJETIVOS ESPECÍFICOS: *Al finalizar el curso el estudiante deberá ser capaz de:*

1. *Entender y explicar los conceptos básicos asociados a los canales de comunicación cuántica y a las redes cuánticas.*
2. *Usar operativamente el concepto de entrelazamiento cuántico, en sus diferentes formas, y su implementación en las comunicaciones cuánticas.*
3. *Calcular analíticamente los parámetros relacionados con la teoría cuántica de la información y sus aplicaciones, en la criptografía cuántica y en las comunicaciones cuánticas.*
4. *Determinar cual son las distribuciones de llaves cuánticas adecuadas para procesos de comunicación cuántica públicos y privados.*
5. *Construir protocolos cuánticos de seguridad asociados a los procesos de transferencia cuántica de información segura.*
6. *Interpretar montajes experimentales básicos de criptografía cuántica y sus aplicaciones*

8. CONTENIDOS

1.- ELEMENTOS DE LA TEORIA DE INFORMACION CUANTICA EN COMUNICACIÓN CUANTICA: Comunicaciones cuánticas bipartitas. Estados entrelazados (en variables discretas, en variables continuas, ortogonales y no ortogonales). Concentración del entrelazamiento. Teorema de la no-clonación. Clonación local de sistemas entrelazados. Teorema de la capacidad cuántica. Teorema de la codificación directa. Entropía y codificación cuántica: Entropía de Shannon, de von Neumann, Rényi, de Bennett y Slutsky.

2.- ELEMENTOS DE COMPUTACION CUÁNTICA: Compuertas cuánticas de un qubit, compuertas controladas y generación de entrelazamiento, compuertas cuánticas universales**.** Codificación densa y teleportación. Modelos alternativos.

3.- FUNDAMENTOS DE COMUNICACIÓN CUÁNTICA: Elementos de las comunicaciones cuánticas. Canales cuánticos de información. Capacidad de un canal cuántico. Fidelidad del canal. Canales cuánticos con memoria y sin memoria. Canales Gaussianos y no Gaussianos. Ruidos y errores en canales cuánticos reales. Decoherencia. Comunicaciones en espacio libre. Redes Cuánticas. Ilustración de los canales cuánticos y redes cuánticas en Óptica Cuántica, Física Nuclear, Computación Cuántica, etc.

4.-PROTOCOLOS DE COMUNICACIÓN CUANTICA: Protocolos basados en conjuntos de estados no ortogonales (ej: BB84, B92, Estados trampa, SARGO4)**.** Protocolos basados en estados entrelazados (ej: EPR, E91). Protocolos con variables continuas (ej: Protocolos con estados comprimidos, Protocolos con estados coherentes: GG02)

5.- CRIPTOGRAFÍA CUÁNTICA: Fundamentos de la criptografía cuántica. Estados entrelazados y criptografía cuántica. Corrección de errores y amplificación de la privacidad.

6.- DISTRIBUCION DE LLAVES CUANTICAS (QKD):

6.1 Cifrado y distribución de claves. Distribución de claves cuánticas públicas y privadas. Teoría de la información y reconciliación de claves. Distribución de llaves en variable continúa con entrelazamiento en el medio. Distribución de llaves cuánticas con sistemas bipartitos y tripartitos de estados coherentes.

6.2 Análisis de seguridad (ataques y vulnerabilidad). Redes de distribución cuántica de llaves. Autenticación y certificación.

7. -COMUNICACIONES CUANTICAS: Análisis de QKD en sistemas de fibras ópticas, en transmisión de información en espacios libres a largas distancias. Nuevas tecnologías.**:** Aplicaciones a sistemas de transmisión de data en procesos electorales, seguridad aeronáutica, seguridad industrial y militar, comunicaciones satelitales, etc.

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. *Investigaciones*
4. *Presentaciones*
5. *Simulaciones computarizadas*
6. *Prácticas de laboratorio demostrativas*

10. ESTRATEGIAS DE EVALUACIÓN.

Se recomiendan las siguientes:

1. *Pruebas escritas*
2. *Pruebas verbales*
3. *Informes de, simulaciones.*
4. *Ejercicios, tareas y/o asignaciones para fuera del aula*
5. *Presentaciones por parte del estudiante*
6. *Solución de problemas*

11. FUENTES DE INFORMACIÓN:

1.- Alexander V. Sergienko, Quantum Communications and Cryptography, Taylor and Francis, 2006

2.- Sandor Imre y Ferenc Balázs , Quantum Computing and Communications: An Engineering Approach, John Wiley and Sons, Ltd, 2005

3.- Gilles Van Assche, Quantum Cryptography and Secret-Key Distillation. Cambridge University Press, 2006

4.- Christian Kollmitzer y Mario Pirk, Applied Quantum Cryptography, Springer-Verlag, Berlin Heidelberg, 2010

5.- Daniel J. Rogers, Broadband Quantum Cryptography, Morgan and Claypool Publishers, 2010.

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

7.- Gunter Mahler and Volker A. Weberrub, Quantum Networks, Springer-Verlag, Berlin Heidelberg, 1998

8.- Nicolas Gisin, Gregoire Ribordy, Wolgang Tittel y Hugo Zbinden, Quantum Cryptography, Review of Modern Physics, Vol. 74 , No 1 (2002) 145-195