UNIVERSIDAD SIMÓN BOLÍVAR
Vicerrectorado Académico

1 .Departamento: *FÍSICA*

2. Asignatura: **CRIPTOGRAFIA CUÁNTICA EMPRESARIAL**

3. Código de la asignatura: **FS-7448**

No. de unidades-créditos: 4

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

4. Fecha de entrada en vigencia de este programa: Enero 2016

5. Requisitos:

6. OBJETIVO GENERAL**:**

Formar a los estudiantes con los conceptos y herramientas básicas necesarias para el entendimiento, simulación, diseño e implementación de procesos de comunicación cuántica segura en el mundo empresarial.

7. OBJETIVOS ESPECÍFICOS:

Al finalizar el curso el estudiante tendrá competencias para:

1. Entender los fundamentos básicos físicos (teóricos y experimentales) y matemáticos de la criptografía cuántica.
2. Dominar algunos de los protocolos de uso más común en criptografía cuántica.
3. Simular algunos protocolos de criptografía cuántica usando un computador convencional.
4. Entender los fundamentos cuánticos básicos de las arquitecturas de redes cuánticas.
5. Dominar los elementos conceptuales y metodológicos básicos para la formulación de proyectos sencillos de comunicación cuántica segura, en procesos de transferencia de información sensible en el área empresarial.

8. CONTENIDO PROGRAMATICO**:**

1.- FUNDAMENTOS DE LA TEORÍA DE INFORMACIÓN CUÁNTICA: Espacios vectoriales, espacios vectoriales duales, matrices de Pauli, descomposición espectral, producto tensorial, qubits. Comunicaciones cuánticas bipartitas, representación de Bloch. Formalismo de la matriz densidad. Trazas parciales. Estados clásicos, cuánticos, producto y entrelazados. Estados puros y estados mixtos. Destilación. Sistemas multipartitos GHZ y W. Medidas de entrelazamiento (sistemas bipartitos y multipartitos). Clasificación de las mediciones. Proyecciones y valores esperados. Localidad y realidad. Paradoja de EPR. Variables ocultas, Desigualdades y Teorema de Bell.

2.- FUNDAMENTOS DE LA COMUNICACIÓN CUÁNTICA: Elementos de las comunicaciones cuánticas. Capacidad de un canal cuántico. Fidelidad del canal. Decoherencia en canales de comunicación cuántica: ecuación maestra para sistemas abiertos, operadores de Krauss. Canales cuánticos con memoria y sin memoria. Teorema de la comunicación directa: Entropías de Shannon, von Neumann y Rény. Teorema de Holevo, Teorema de la no-clonación. Clonación local de sistemas entrelazados.

3.-ELEMENTOS DE COMUNICACIÓN CUÁNTICA: Compuertas cuánticas de un qubit, compuertas controladas y generación de entrelazamiento, compuertas cuánticas universales. Alfabeto cuántico. Distribución de claves cuánticas (QKD), públicas o privadas. Codificación densa y Teleportación.

4.- PROTOCOLES DE CRIPTOGRAFÍA CUÁNTICA:

4.1.- **Protocolos basados en conjuntos de estados ortogonales:** BB84, B92, Estados trampa, SARG04, Ping-pong, estados decodificados, DPS, COW, S09 y S13.

4.2.- **Protocolos basados en estados entrelazados**: E91, protocolos cuánticos de comparación privada usando estados y medidas de Bell. Protocolo de acuerdo de llave cuántica con estados clúster.

4.3.- **Protocolos con variables continuas**: Protocolos con estados coherentes bipartitos (GC02) y tripartitos. Protocolos con entrelazamiento y empate en el medio.

4.4.- **Simuladores de protocolos cuánticos:** Aplicaciones al BB84 y E91

5.- 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.

6.- 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. Internet Cuántico.

7.- 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.

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/o 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 el mundo empresarial, y la formulación de propuestas para resolverlos usando los conocimientos aprendidos en el curso.
6. Formulación de propuestas originales y rigurosas de protocolos criptográficos, o de arquitecturas de redes de comunicación cuántica que sean novedosas, que optimicen o mejoren las ya conocidas
7. Formulación de proyectos que contemplen el diseño, implementación y seguimiento, que permitan resolver situaciones reales de seguridad empresarial.

11. FUENTES DE INFORMACIÓN:

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

2,. Van Meter, "Quantum Networking", Kindle Edition, Jhon Wiley and Sons, (2014)

3.- Song Y. Yan, "Quantum Attacks on Public-Key Cryptosystems", Springer New York Heidelberg Dordrecht London. (2013)

4.- Mark M. Wilde, "Quantum Information Theory", McGill University, Montréal (2013)

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

6.- Daniel J. Rogers, Broadband Quantum Cryptography, Morgan and Claypool Publishers, (2010).

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

8.- Daniel J. Bernstein · Johannes Buchmann Erik Dahmen, "Post-Quantum Cryptography", Springer-Verlag Berlin Heidelberg (2009)

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

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

11.- Alexander V. Sergienko, Quantum Communications and Cryptography, Taylor and Francis, (2006)