UCAB Universidad Católica ANDRÉS BELLO
Escuela de Ingeniería Informática

PROGRAMA DE ASIGNATURA

I.- DATOS GENERALES

Nombre de la Carrera o Programa: Ingeniería Informática

Nombre de la Asignatura: Seguridad Computacional

Departamento: Departamento de Telemática

Régimen: Semestral	**Número de Unidades Crédito:** 5
Ubicación en el plan de estudios: Noveno Semestre	
Requisitos: Redes de Computadores I	**Asignaturas a las que aporta:** -

Tipo de asignatura:

Obligatoria: X	Electiva:

Horas semanales:

Teoría: 2	Práctica: 0	Laboratorio: 2

Vigente desde: Octubre 2015

II.- JUSTIFICACIÓN

La apertura de los sistemas computacionales, gracias a las facilidades de conexiones remotas, es producto de las ventajas que ofrecen las redes informáticas. Sin embargo, este beneficio impone la necesidad de controles para: proteger los datos, verificar la identidad del usuario y asegurar el correcto funcionamiento de los programas. Ante esta realidad, la unidad curricular Seguridad Computacional persigue la formación de ingenieros en informática competentes en el diseño y desarrollo de sistemas de redes seguros y aplicaciones de software confiables. La función del ingeniero en informática es evitar que los usuarios sufran de atentados contra la privacidad de la información, suplantaciones de identidad o modificaciones de sus datos. El usuario deposita su confianza en el ingeniero en informática por lo que el manejo ético de la información confidencial por parte del ingeniero es fundamental, ya que, es el responsable de la seguridad de sus clientes. La seguridad computacional dentro del plan de estudios se complementa con las unidades curriculares de redes de computadores, arquitectura del computador y sistemas de operación. Es por ello que resulta indispensable trabajar en grupos interdisciplinarios donde además de dominar aspectos técnicos deben tomarse en cuenta aspectos psicológicos. El factor humano en el área de seguridad, en general, es vital ya que es un proceso incómodo en el que el usuario debe aceptar las imposiciones que implican un ambiente de trabajo seguro y confiable. A fin de cuenta el ingeniero debe hacer sentir al usuario seguro y confiado de la tecnología que utiliza.

III.- CONTRIBUCIÓN DE LA ASIGNATURA AL DESARROLLO DE LAS COMPETENCIAS

Competencia General 1 (CG1): Aprender a aprender con calidad	
Unidad de Competencia 1 (CG1 - U1): Aplica los conocimientos de la práctica	**Criterios de desempeño de la U1:** 1. Implementa el proceso a seguir para alcanzar los objetivos mediante acciones, recursos y tiempo disponible 2. Evalúa los resultados obtenidos
Unidad de Competencia 2 (CG1 - U2): Demuestra conocimiento sobre su área de estudio y profesión	**Criterios de desempeño de la U2:** 1. Aplica los procedimientos de la disciplina para resolver problemas y aportar soluciones
Competencia General 2 (CG2): Aprender a trabajar con el otro	
Unidad de Competencia 1 (CG2 - U1): Participa y trabaja en equipo	**Criterios de desempeño de la U1:** 1. Realiza las tareas establecidas por el equipo
Competencia Profesional Básica 1 (CPB1): Formula Proyectos de Ingeniería	
Unidad de Competencia 1 (CPB1 - U1): Cumple con el código de ética profesional y el marco legal vigente	**Criterios de desempeño de la U1:** 1. Diferencia casos que están fuera de la ética profesional en la ingeniería 2. Aplica el código de ética en su ambiente profesional
Competencia Profesional Específica 1 (CPE1): Desarrolla sistemas telemáticos	
Unidad de Competencia 1 (CPE1 - U1): Diseña e implementa sistemas de seguridad en redes	**Criterios de desempeño de la U1:** 1. Selecciona y aplica políticas de seguridad en una red 2. Instala y configura herramientas para la creación de una red segura
Unidad de Competencia 2 (CPE1 - U2): Administra y mantiene sistemas operativos	**Criterios de desempeño de la U2:** 1. Aplica comandos para el manejo de diferentes sistemas operativos 2. Utiliza las herramientas para el manejo de sistemas operativos
Competencia Profesional Específica 2 (CPE2): Desarrolla software de aplicación	
Unidad de Competencia 1 (CPE2 - U1): Analiza las necesidades de los usuarios, diseña e implementa el software de aplicación sobre arquitecturas centralizadas o distribuidas	**Criterios de desempeño de la U1:** 1. Diseña la solución planteada 2. Implementa la solución planteada

IV.- UNIDADES TEMÁTICAS

UNIDADES	TEMAS
1. Principios y conceptos básicos de seguridad	**Teoría** 1.1. Características de un sistema seguro 1.2. Principios de hacking benéfico 1.3. Estrategias de respeto al copyright usando copyleft 1.4. Definición de políticas de seguridad (Teoría) **Laboratorio** 1.5. Principios básicos de un sistema operativo de código abierto
2. Criptografía simétrica y de clave pública	**Teoría** 2.1. Principios de cifrado simétrico y asimétrico o de clave pública 2.2. Propiedades de los algoritmos de clave pública 2.3. Algoritmos de negociado de clave simétrica 2.4. Mecanismo de cifrado irreversible 2.5. Desafíos de la seguridad en mercados competitivos **Laboratorio** 2.6. Comandos básicos de seguridad en sistemas operativos de código abierto 2.7. Comandos de conexión y transferencia de archivos segura (Laboratorio)
3. Autentificación y firma digital.	**Teoría** 3.1. Algoritmos de autentificación con clave simétrica 3.2. Autentificación con centros de claves o KDC 3.3. Autentificación con algoritmos de hash 3.4. Autentificación con algoritmos de clave pública 3.5. Principios de firma digital **Laboratorio** 3.6. Generar claves públicas y privadas para cifrar y firmar documentos
4. Certificación digital	**Teoría** 4.1. Infraestructura de certificación digital o PKI 4.2. Tipos de Autoridades de Certificación y estampillado digital 4.3. Problemas de las normas de revocación de certificados 4.4. Tipo de certificados 4.5. Problemas legales y técnicos de la infraestructura PKI 4.6. Certificados digitales con autoridad de certificación distribuida 4.7. Revocación de claves públicas con certificación distribuida 4.8. Manejo de claves públicas y privadas por repositorio 4.9. Confianza de las claves públicas **Laboratorio** 4.10. Infraestructura local de certificación y firma digital (gpg) 4.11. Manejo de claves públicas y privadas por repositorio 4.12. Confianza de las claves públicas 4.13. Generación y autofirma de certificados digitales 4.14. Instalación de servidor Web con certificados de ambos actores: cliente y servidor 4.15. Instalación de servidor Web con certificados de ambos actores: cliente y servidor

IV.- UNIDADES TEMÁTICAS

UNIDADES	TEMAS
5. Seguridad en redes	**Teoría** 5.1. Modelo de capas seguras para aplicaciones en red 5.2. Modalidades de pago electrónico. Gobierno electrónico seguro 5.3. Protección de canales mediante redes privadas virtuales o VPN 5.4. Inspección de redes con sistemas de detección de intrusos 5.5. Servidores de dominio seguros 5.6. Seguridad en las redes inalámbricas 5.7. Filtrado de información a través de cortafuegos 5.8. Programación de aplicaciones cliente/servidor seguras 5.9. Librerías seguras para montar enlaces cifrados con autentificación **Laboratorio** 5.10. Filtrado de información a través de cortafuegos 5.11. Programación de aplicaciones cliente/servidor seguras 5.12. Librerías seguras para montar enlaces cifrados con autentificación
6. Ataques y medidas preventivas y correctivas	**Teoría** 6.1. Tipos particulares de ataques: virus, troyanos, gusanos, spywares y otras amenazas 6.2. Técnicas de hacking benéfico 6.3. Fases de la informática forense **Laboratorio** 6.4. Fases de la informática forense 6.5. Inspección y auditoría de redes para hacking benéfico

V.- ESTRATEGIAS DE ENSEÑANZA Y DE APRENDIZAJE

Clases magistrales con presentación de casos de estudio, Visualización de películas y lectura de libros o artículos en el área de seguridad asociado a evaluaciones críticas y de discusión, Demostraciones de la infraestructura tecnológica local y en redes, Talleres tipo cuestionario para resolver ejercicios práctico de seguridad y redes, Proyecto de envergadura para aplicar técnicas de diseño y desarrollo de sistemas seguros

VI.- ESTRATEGIAS DE EVALUACIÓN

Pruebas escritas, Cuestionarios de laboratorios, Proyectos individuales y en grupos, Trabajos críticos

VII.- REFERENCIAS BIBLIOGRÁFICAS

Textos:

1. Stallings, W. *Fundamentos de Seguridad en Redes: Aplicaciones y Estándares* (2da ed.). Prentice Hall.
2. Garfinkel, S. & Spafford, G. *Seguridad y Comercio en la Web*. O'Reilly Media.
3. Cariacedo, J. *Seguridad en Redes Telemáticas*. McGraw-Hill.
4. Hatch, B., Lee, J. & Kurtz, G. *Hackers en Linux: Secretos y Soluciones para la Seguridad en Linux*. Osborne y McGraw-Hill.
5. Cano, J. *Computación Forense: Descubriendo los Rastros Informáticos* (2da ed.). Alfaomega.

Web:

1. http://www.phrack.org
2. http://www.debianhackers.net
3. http://www.dragonjar.org
4. http://seguridadyredes.wordpress.com
5. http://foro.elhacker.net
6. http://blog.elhacker.net
7. http://warzone.elhacker.net
8. http://www.sleuthkit.org