PROGRAMA DE MATERIA

DATOS DE IDENTIFICACIÓN

MATERIA:	**OPTATIVA PROFESIONALIZANTE – SEGURIDAD EN COMPUTO**				
CENTRO ACADÉMICO:	CIENCIAS BÁSICAS				
DEPARTAMENTO ACADÉMICO:	SISTEMAS ELECTRÓNICOS				
PROGRAMA EDUCATIVO:	INGENIERO EN SISTEMAS COMPUTACIONALES				
AÑO DEL PLAN DE ESTUDIOS:	2016	**SEMESTRE:**	8°	**CLAVE DE LA MATERIA:**	28722
ÁREA ACADÉMICA:	REDES Y COMUNICACIONES		**PERIODO EN QUE SE IMPARTE:**	ENERO-JULIO	
HORAS SEMANA T/P:	2/2		**CRÉDITOS:**	6	
MODALIDAD EDUCATIVA EN LA QUE SE IMPARTE:	PRESENCIAL		**NATURALEZA DE LA MATERIA:**	OPTATIVA	
ELABORADO POR:	SGC, FGGN, LEBV				
REVISADO Y APROBADO POR LA ACADEMIA DE:	REDES Y PROGRAMACIÓN DE SISTEMAS		**FECHA DE ACTUALIZACIÓN:**	ENERO 2021	

DESCRIPCIÓN GENERAL

En los sistemas computacionales actuales existe una interconexión casi natural entre ellos y con otros a través de Internet. Aun si existe la diversidad de sistemas computacionales es posible integrarlos sin dejar de lado la seguridad. Los peligros que puede presentar una conexión hacia el exterior son muy importantes, puesto que los sistemas (con todo lo que ello conlleva: recursos de cálculo, de espacio en disco, datos confidenciales, etc.) estarán expuestos a millones de personas. Las estadísticas recogen que el número de incidentes de seguridad se duplica cada año, no incrementándose las inversiones realizadas en aspectos de seguridad en la mayoría de las instituciones..

Las herramientas de seguridad informática son un elemento importante para que los administradores de las TICs puedan gestionar y controlar eficientemente las aplicaciones que utilizan los usuarios: recursos de cálculo, de espacio en disco, datos confidenciales, etc.) estarán expuestos a millones de personas. Las aplicaciones recogen que el número de incidentes de seguridad se duplica cada año, no incrementándose las inversiones realizadas en aspectos de seguridad en la mayoría de las instituciones.

OBJETIVO (S) GENERAL (ES)

El estudiante identificará e interpretará la importancia de la seguridad y las herramientas inteligentes de seguridad, e identificará los distintos riesgos a los que están expuestos los sistemas y redes de computadoras.

Además, aplicará los principios de la protección de sistemas de software contra el acceso no autorizada o la modificación de información, contra la negación y acceso a servicios a los usuarios según sus categorías y, empleará y creará herramientas inteligentes para la detección y reducción de riesgos.

.

*En caso de no aplicar algún elemento, escribir **N/A**

Código: FO-030200-13
Revisión: 02
Emisión: 13/12/11

CONTENIDOS DE APRENDIZAJE

UNIDAD TEMÁTICA I: INTRODUCCIÓN A LA SEGURIDAD (10 horas aprox.)		
OBJETIVOS PARTICULARES	**CONTENIDOS**	**FUENTES DE CONSULTA**
Comprender el fundamento y necesidad de la implementación de modelos de seguridad	1. Introducción a la Seguridad y sus Conceptos 1.1. Triángulo de seguridad de Información 1.1.1. Confidencialidad 1.1.2. Disponibilidad 1.1.3. Integridad 1.2. Confiabilidad en Equipos y Comunicaciones 2. Amenazas, Vulnerabilidades y Esquemas de Defensa 2.1. El enemigo y sus motivos 2.2. Puntos de Vulnerabilidad 2.3. Tipos de Amenazas 2.4. Esquemas de Defensa 2.5. Introducción a Ethical Hacking 2.6. Ethical Hacking en Monitoreo	1,2,4,5

UNIDAD TEMÁTICA II: SEGURIDAD EN LA INFRAESTRUCTURA DE RED (25 horas aprox.)		
OBJETIVOS PARTICULARES	**CONTENIDOS**	**FUENTES DE CONSULTA**
Comprender los aspectos de seguridad implementados en las redes de computadoras y sus protocolos.	1. Seguridad en las Redes de Computadoras 1.1. Comunicaciones y Canales Seguros 1.2. Protocolos y Mensajes Seguros 1.3. Aplicaciones y Servicios Seguros 2. Arquitectura Segura en Internet 2.1. Espacio e Integración de la Seguridad 2.2. Modelos de Cómputo Seguro 2.3. IP v4 vs. IP v6 2.4. TCP, UDP y Capas Superiores 2.5. Túneles 3. Protocolos Seguros y de Seguridad 3.1. IPSEC 3.2. SSL/TSL 3.3. HTTPS 3.4. SSH 3.5. Kerberos 3.6. Autoridades Certificadoras 4. Aplicaciones Seguras 4.1. Firewalls y sus Arquitecturas 4.2. Autentificación y Autorización 4.3. ACLs 4.4. Filtrado y Suavizado de Paquetes	2,3,4,5

*En caso de no aplicar algún elemento, escribir **N/A**

	4.5. Proxies y Bastiones 4.6. NAT 5. Controles para el Acceso y el Uso 5.1. Identificación e Identidad 5.2. Acceso: Controles y Permisos 6. Bitácoras del uso de la red	

UNIDAD TEMÁTICA III: COMUNICACIONES SEGURAS (10 horas aprox.)		
OBJETIVOS PARTICULARES	**CONTENIDOS**	**FUENTES DE CONSULTA**
Comprender los elementos y su implementación de una comunicación segura a través de una red de cómputo.	1. Estenografía 2. Criptografía y Criptoanálisis 2.1. Tipos de comunicaciones 2.1.1. Interrupción, interceptación, falsificación, generación 2.2. Escondiendo el sentido del mensaje 2.3. Llaves Únicas vs. Públicas y Privadas 2.4. Criptografía de bloque y de flujo 2.4.1. Lucifer, DES, 3DES, Loki, Blowfish 2.5. Protocolos 2.5.1. MD5 2.5.2. SHA1 2.5.3. RSA y SSL 2.6. Firmas electrónicas	

UNIDAD TEMÁTICA IV: APLICACIONES DE SEGURIDAD (15 horas aprox.)		
OBJETIVOS PARTICULARES	**CONTENIDOS**	**FUENTES DE CONSULTA**
Comprender los aspectos básicos relacionados con la ocurrencia de ataques a la seguridad y a las herramientas utilizadas para ello	1. Ética de hackeo 1.1. Hackeo Ético 1.2. Hackeo de Control 1.3. Crackeo 2. Ataques en Sistemas Microsoft 2.1. Virus, Troyanos, Malware y Gusanos 2.2. Ataques a Contraseñas 2.3. Ataques a las Directivas 2.4. Ataques al Directorio Activo 2.5. Ataques a los Servicios Integrados 3. Ataques en Sistemas UNIX 3.1. Gusanos y Rootkits 3.2. DoS y DDoS 3.3. Ataques a Contraseñas 3.4. Enmascaramiento de Identidad 3.5. Ataques a los Servicios 4. Herramientas de Defensa en Sistemas UNIX 4.1. Endurecimiento de las Defensas 4.2. Detección de Intrusos	2,3,4

*En caso de no aplicar algún elemento, escribir **N/A**

	4.3. Herramientas de Análisis del Tráfico 5. Herramientas de Descubrimiento de las Redes	

UNIDAD TEMÁTICA V: SEGURIDAD INTELIGENTE (20 horas aprox.)		
OBJETIVOS PARTICULARES	**CONTENIDOS**	**FUENTES DE CONSULTA**
Describir y aplicar las mejores metodologías conocidas para incrementar los niveles de seguridad aplicadas a las redes de computadoras	1. La Administración y la Seguridad Informática 1.1. Sistemas de administración de la seguridad 1.2. Monitoreo de seguridad / intrusiones 2. Actividades de Control a la Seguridad 2.1. Atención a incidentes 2.2. Auditorias de seguridad 2.3. Seguridad perimetral 2.4. Pruebas de penetración 3. Rastreo de Ataques 3.1. Ataques comprobados y detección de fuentes 3.2. Análisis forense 3.3. Deslinde y Aplicación de Responsabilidades 4. Plan de Contingencias 4.1. Niveles y Planes de Contingencia 5. Evaluación de Riesgos	1,2,3,4,5

METODOLOGÍA DE ENSEÑANZA - APRENDIZAJE

- Exposiciones teóricas verbales y gráficas por parte del profesor.
- Trabajos de investigación e instalaciones por parte de los alumnos.
- Lecturas e investigaciones referentes a seguridad de sistemas, seguridad en redes, seguridad en aplicaciones.
- Proyectos de desarrollo que apliquen la teoría por parte de los alumnos.
- Asistencia a Simposios y Congresos donde se trate el tema.
- Asesorías sobre temas de clase y asociados por parte del profesor.
- Visitas guiadas a organizaciones en donde se tengan implementados sistemas de seguridad.

RECURSOS DIDÁCTICOS

- Aula de clases y pizarrón.
- Laboratorio de equipo de cómputo, con equipamiento audiovisual.
- Laboratorio con equipo de interconectividad de redes, simuladores de redes.
- Bibliografía y sitios Web.
- Videos alusivos al tema.
- Instalaciones en organizaciones que emplean dichos sistemas.

*En caso de no aplicar algún elemento, escribir **N/A**

- Plataforma de Educación a Distancia (Moodle).

EVALUACIÓN DE LOS APRENDIZAJES

Criterio	Porcentaje	Componentes	Contenidos
Parcial I	25%	• Examen	Unidades 1, 2
Parcial II	25%	• Examen	Unidades 2, 3
Parcial III	25%	• Examen	Unidades 4, 5
Proyecto Final (práctico)	25%	• Portada 5% • Índice 5% • Introducción 5% • Contenido 60% • Conclusiones 20% • Bibliografía 5%	Proyecto de seguridad para múltiples computadoras locales y remotas con esquemas de control y monitoreo. Presentarlo hasta el examen final.
Tareas, prácticas, exposiciones e investigaciones (teórica)	Distribuido entre parciales	• Presentación • Inducción • Contenido • Conclusiones • Bibliografía	Todas las unidades e investigaciones de temas afines. Presentar reportes (antes de cada examen o cuando el profesor los requiera).

Condiciones:

- Para acreditar el curso, se deberá de aprobar con una mínima aprobatoria del 70%.
- Para tener derecho a presentar examen final, se deberá tener una asistencia mínima del 80% del tiempo de clases.
- El proyecto final se calificará en equipo y en forma individual; es decir, cada integrante del equipo tendrá su propia calificación del proyecto y no forzosamente debe ser la misma para todos los integrantes.

NOTAS PARA EL DOCENTE:

1. La calificación de cada parcial se integra de actividades sumativas adicionales al examen, las calificaciones de estas actividades se reportarán un viernes antes del comienzo del parcial
2. La calificación final de cada parcial integrada por la ponderación de todas las actividades incluido el examen será reportada en el sistema de acuerdo como marca el reglamento (7 días naturales a partir del fin del período)

FUENTES DE CONSULTA

BÁSICAS:

1. Hacking Exposed, 6th Edition, Stuart McClure, McGraw-Hill Ubicación en Biblioteca 005.8M1287h21
2. Pellejero Izakun, “Fundamentos y aplicaciones de seguridad en redes WLAN”, Macombo, 2006. Ubicación en Biblioteca 005.8P386f 21.
3. Newman, Robert C., “Computer Security: protecting digital resources”, Jones & Barlett Publishers, 2010. Ubicación en Biblioteca 005.8N554c22
4. R. Rowlingson Robert, “Essential Guide to Home Computer Security”, British Informatics Society, 2011. Disponible en e-brary https://site.ebrary.com.dibpxy.uaa.mx/lib/univeraguascalientes/docDetail.action?docID=10582850&p00=cisco%2security

COMPLEMENTARIAS:

*En caso de no aplicar algún elemento, escribir **N/A**

5. Osborn Mark, “How to Cheat at Managing Information Security”, Syngress Publishing, 2006. Disponible en e-brary https://site.ebrary.com.dibpxy.uaa.mx/lib/univeraguascalientes/docDetail.action?docID=107836550&p00=cisco%2security
6. Mowbray Thomas L., “Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions”, Jhon Wiley & Sons, 2013. Disponible en e-brary https://site.ebrary.com.dibpxy.uaa.mx/lib/univeraguascalientes/docDetail.action?docID=1014561&p00 =security

OTRAS FUENTES:

7. Fundamentos de Seguridad en Redes, 1a Edición, CISCO Press & Pearson Educación
8. Fundamentos de Seguridad de Redes, 2a Edición, Maiwald, Mc-Graw Hill
9. Seguridad En Redes Informáticas, 1a Edición, Justo Carracedo, Mc-Graw Hill
10. Fundamentos de Seguridad en Redes, 2a Edición, William Stallings, Pearson Educación
11. An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12