DATOS DE IDENTIFICACIÓN

MATERIA:	SEGURIDAD DE SISTEMAS				
CENTRO ACADÉMICO:	CIENCIAS BÁSICAS				
DEPARTAMENTO ACADÉMICO:	SISTEMAS ELECTRÓNICOS				
PROGRAMA EDUCATIVO:	LICENCIADO EN INFORMATICA Y TECNOLOGIAS COMPUTACIONALES				
AÑO DEL PLAN DE ESTUDIOS:	2014	SEMESTRE:	8°	CLAVE DE LA MATERIA:	22436
ÁREA ACADÉMICA:	REDES Y COMUNICACIONES		PERIODO EN QUE SE IMPARTE:	ENERO – JUNIO 2021	
HORAS SEMANA T/P:	3/2		CRÉDITOS:	8	
MODALIDAD EDUCATIVA EN LA QUE SE IMPARTE:	PRESENCIAL		NATURALEZA DE LA MATERIA:	OBLIGATORIA	
ELABORADO POR:	LEBV, AER				
REVISADO Y APROBADO POR LA ACADEMIA DE:	REDES Y PROGRAMACIÓN DE SISTEMAS		FECHA DE ACTUALIZACIÓN:	ENERO 2021	

DESCRIPCIÓN GENERAL

Este curso está dirigido a los estudiantes de Licenciado en Informática y Tecnologías Computacionales y tiene como objetivo el dar una visión de los distintos problemas de seguridad y privacidad que se pueden producir en las tecnologías de información, así como una introducción a los métodos, procedimientos y técnicas que han sido generados para solucionar cada uno de ellos, lo que permite afrontar de forma eficaz la mejora de la seguridad aplicada a tecnologías de información.

Se trata de un curso teórico-práctico de carácter presencial, mediante el cual el estudiante comprenderá los fundamentos, las políticas y las amenazas dentro de los esquemas de seguridad, para su implantación y administración en los sistemas informáticos y redes de cómputo. Esta materia tiene como precedentes a Principios de Informática, Arquitectura de Computadoras, Ingeniería de Requerimientos y Análisis de Riesgos, Elementos de Derecho Informático, Organización Computacional, Sistemas Operativos y Redes Informáticas y es antecedente de Administración de la Función Informática.

OBJETIVO (S) GENERAL (ES)

Al finalizar el curso el participante entenderá los aspectos involucrados en la administración y las políticas de seguridad de los sistemas de información.

Objetivos Particulares:

1. Implantar y gestionar medidas de seguridad ante posibles ataques o actividades inapropiadas de usuarios de sistemas de información.
2. Evaluar riesgos y garantizar la confidencialidad y la integridad de los datos y las comunicaciones en los sistemas computacionales dentro de las organizaciones.

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

UNIDAD I: Fundamentos de Seguridad (20 hrs.)		
OBJETIVOS PARTICULARES	**CONTENIDOS**	**FUENTES DE CONSULTA**
Comprender el fundamento y necesidad de la implementación de modelos de seguridad.	1. Introducción al triangulo de Seguridad de Información 1.1. Confidencialidad 1.2. Disponibilidad 1.3. Integridad 2. Controles para el Acceso y el Uso 2.1. Identificación e Identidad 2.2. Contraseñas (NIST Recomendaciones) 2.3. Autentificación de múltiples factores 2.4. Acceso: Controles y Permisos 3. Amenazas, Vulnerabilidades y Esquemas de Defensa 3.1. El enemigo y sus motivos 3.2. Tipos de Amenazas 3.3. Esquemas de Defensa 3.4. Introducción al Ethical Hacking	2,1

UNIDAD II: Introducción a la criptografía y certificados (10 hrs.)		
OBJETIVOS PARTICULARES	**CONTENIDOS**	**FUENTES DE CONSULTA**
Comprender la importancia de la criptografía y principales métodos criptográficos.	1. Introducción a la Criptografía 2. Criptografía Simétrica 2.1. Criptografía de bloque 2.1.1. 3DES, AES, Twofish 2.2. Criptografía de flujo 2.2.1.RC4 (WEP, SSL, WPA) 3. Criptografía Asimétrica 3.1. RSA, Firmas electrónicas 4. Funciones Hash 4.1. MD5, SHA 5. Certificados 5.1. Autoridades certificadoras 5.2. Creación de certificados Estenografía	3,2

UNIDAD III: Infraestructura de Seguridad (15hrs.)		
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. Protocolos Seguros y de Seguridad 2.1. IPSEC – VPN (Tunneling) 2.2. SSL/TSL 2.3. HTTP vs HTTPS 2.4. FTP vs SFTP	1, 2, 3,4

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

	2.5. Telnet vs SSH 2.6. Kerberos 2.7. The onion router (TOR) 3. Dispositivos de Red 3.1. Firewalls (Fisicos y de aplicación) 3.2. Access Control Lists (ACLs) 3.3. Filtrado y Suavizado de Paquetes 3.4. Proxies y Bastiones 3.4.1.NAT 3.5. IDS	

UNIDAD IV: Seguridad aplicaciones y física (10hrs.)		
OBJETIVOS PARTICULARES	**CONTENIDOS**	**FUENTES DE CONSULTA**
Comprender los aspectos de seguridad relacionados con el manejo y tratamiento de la información y sus entornos fisicos.	4. Seguridad de aplicaciones 4.1. Open Web Application Security Project (OWSAP) 4.2. Cross-Site Scripting (XSS) 4.3. Inyección SQL 4.4. Ingeniería inversa 5. Seguridad física 5.1. Controles de acceso fisicos 5.2. Cámaras y sensores 5.3. Tailgaiting Lockpicking	2,3

UNIDAD V: Administración de la Seguridad de Información (15 hrs.)		
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 de Información 1.1. Business Continuity Plan 1.2. Impacto en el negocio 2. Monitoreo de seguridad / intrusiones 2.1. Reportes de Vulnerabilidad 2.2. Grado de Vulnerabilidad 3. Atención a incidentes 3.1. Disasrter Recovery Plan 3.2. Legislación Informática 4. Auditorias de seguridad. 4.1. Bitácoras. 4.2. Deslinde y Aplicación de Responsabilidades	1,2,3

METODOLOGÍA DE ENSEÑANZA - APRENDIZAJE

El curso es de naturaleza teórico--práctica y será impartido en modalidad en presencial en el periodo ordinario de cursos establecido por el consejo universitario, en el aula asignada y los laboratorios de redes del edificio 204 y/o 54, con soporte de actividades en línea, utilizando un espacio en la Plataforma moodle e--Academia, del Centro de

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

Ciencias Básicas, o en el de Aula Virtual institucional según lo determine el docente, mediante la implementación de las siguientes actividades:

- Realización de exposiciones teóricas verbales y gráficas por parte del profesor.
- Uso de TICs que permitan al alumno una mayor interacción y comprensión de la parte conceptual de la materia.
- Implementación de sesiones semipresenciales mediante alguna plataforma de educación a distancia (Moodle).
- Realización de trabajos e investigaciones por parte de los alumnos.
- Instalaciones y configuración de redes de cómputo en laboratorio y simuladores.
- Realización de proyectos que apliquen la teoría por parte de los alumnos. (De forma individual o en equipos previamente asignados).
- Asistencia a Simposios y Congresos donde se trate el tema.
- Visitas guiadas a organizaciones donde se cuente con redes de computadoras.
- Los objetivos del curso se atenderán a través de la combinación de estrategias centradas en el profesor (exposición oral, interrogación didáctica y demostración) y estrategias centradas en el estudiante (Método de proyectos, aprendizaje basado en problemas y estudio de casos), según la experiencia docente en la implementación de estas estrategias.
- Se privilegiará un esquema de trabajo colaborativo, ya sea en forma individual, de equipo o grupal.
- La evaluación se realizara a través del enfoque diagnóstico, motivacional, formativo y sumativo

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.
- Plataforma de Educación a Distancia (Moodle).

EVALUACIÓN DE LOS APRENDIZAJES

La evaluación diagnóstica se realizará con un cuestionario para explorar el aprendizaje afectivo alcanzado por los alumnos en los cursos previos que son base a la materia, identificando las debilidades y fortalezas del grupo para poder determinar los alcances del curso.
La evaluación motivadora se realizará en base a prácticas de laboratorio y estudios de casos que permitan al alumno comprobar los progresos con respecto a los objetivos del curso.
La evaluación formativa se llevará a cabo a través del seguimiento y la retroalimentación permanente a las participaciones y producciones generadas por el estudiante.
El valor de los procesos de evaluación se enuncia a continuación.

Criterio	Porcentaje	Componentes	Contenidos
Parcial I	25 %	1. Examen y trabajos	Unidades 1, 2
Parcial II	25 %	2. Examen y trabajos	Unidades 2, 3
Parcial III	25 %	3. Examen y trabajos	Unidades 4, 5
Proyecto final (práctico)		Portada 5% Índice 5% Introducción 5%	Proyecto de seguridad para múltiples

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

	25 %	Contenido 60% Conclusiones 20% Bibliografía 5%	computadoras locales y remotas con esquemas de control y monitoreo.
Tareas, exposiciones e investigaciones (teóricas)	Evaluados dentro de cada parcial	• 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).

La evaluación sumativa se dará en términos a las siguientes 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 según su participación 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
2. Fundamentos de Seguridad en Redes, 2a Edición, William Stallings, Pearson Educación
3. An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12

COMPLEMENTARIAS:

4. Fundamentos de Seguridad en Redes, 1a Edición, CISCO Press & Pearson Educación
5. Fundamentos de Seguridad de Redes, 2a Edición, Maiwald, Mc-Graw Hill
6. Seguridad En Redes Informáticas, 1a Edición, Justo Carracedo, Mc-Graw Hill

Otras Fuentes de Información:

1. *The 60 minute network security guide: First steps towards a secure network environment*. 2002. Ft. Mead, MD: National Security Agency, sd-7. Available from http://nsa2.www.conxion.com/support/guides/sd-7.pdf.
2. *Principles to guide efforts to improve computer and network security for higher education*. 2003. EDUCAUSE/Internet2 Computer and Network Security Task Force, SEC0310. Available from http://www.educause.edu/asp/doclib/abstract.asp?ID=SEC0310.
3. *Computer access, privacy, and security: Legal obligations and liabilities*. 2003. EDUCAUSE. Accessed April 2 2004. Available from http://www.educause.edu/asp/doclib/abstract.asp?ID=SEC0311.

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

4. *Information and computer security resources*. 2004. SANS: SysAdmin, Audit, Network, Security Institute. Accessed April 7 2004. Available from http://www.sans.org/resources/.
5. *Security resources*. 2004. EDUCAUSE. Accessed April 1 2004. Available from http://www.educause.edu/security/resources.asp.
6. *[Shibboleth Introduction]*. March 2004. Internet 2 Middleware Architecture Committee for Education. Accessed April 7 2004. Available from http://shibboleth.internet2.edu/docs/shibboleth_intro.pdf.
7. Becker, Phil. Aug. 5 2002. *Shibboleth: Identity the internet way*. Digital Identity World. Accessed April 1 2004. Available from http://www.digitalidworld.com/article.php?id=90.
8. Ekhaml, Leticia. 2001. Protecting yourself from internet risks, threats, and crime. *Journal of Educational Media and Library Sciences* 39, no. 1: 8-14.
9. Williams, Robert L. 2001. *Computer and network security in small libraries: A guide for planning*. Texas State Library & Archives Commission. Accessed Apr 5 2004. Available from http://www.tsl.state.tx.us/ld/pubs/compsecurity/.

Sitios:
http://www.metasploit.com/
http://www.backtrack-linux.org/