UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
COORDINACIÓN DE FORMACIÓN BÁSICA
COORDINACIÓN DE FORMACIÓN PROFESIONAL Y VINCULACIÓN UNIVERSITARIA
PROGRAMA DE UNIDAD DE APRENDIZAJE

I. DATOS DE IDENTIFICACIÓN

1. Unidad Académica: Facultad de Ciencias

2. Programa (s) de estudio: Licenciatura en Ciencias Computacionales 3. Vigencia del plan: _____

4. Nombre de la Unidad de aprendizaje: **Seguridad en Cómputo** 5. Clave: _____

6. HC: 2 HL 3 HT 0 HPC ____ HCL ____ HE 2 CR 7

7. Etapa de formación a la que pertenece: terminal

8. Carácter de la Unidad de aprendizaje: Obligatoria ___x____ Optativa _____

9. Requisitos para cursar la unidad de aprendizaje:

Formuló: Evelio Martínez Martínez

Vo.Bo. Dr. Alberto Leopoldo Morán y Solares

Fecha: Noviembre de 2016

Cargo: Subdirector

II. PROPÓSITO GENERAL DE LA UNIDAD DE APRENDIZAJE

Aplicar las nociones fundamentales de la seguridad en redes de cómputo para diseñar esquemas de red seguros, proteger información sensible, configurar servicios de red seguros y administrar redes seguras utilizando herramientas de distribución libre. La unidad de aprendizaje servirá como introducción para que el estudiante pueda instalar y configurar herramientas más utilizadas en el ámbito del software libre. Además, el estudiante estará preparado para resolver situaciones y/o problemas reales.

La asignatura de Seguridad en Cómputo es obligatoria y pertenece a la etapa terminal. Le anteceden las asignaturas de sistemas operativos y redes de datos. Las asignaturas consecuentes relacionadas con ésta son sistemas distribuidos (obligatoria), arquitecturas de protocolos de red, administración de centros de cómputo y otras materias optativas.

III. COMPETENCIA DE LA UNIDAD DE APRENDIZAJE

Diseñar un modelo de seguridad que considere el monitoreo del status actual de la red y los métodos de seguridad de los datos utilizando las herramientas de seguridad de código abierto para mantener las condiciones de integridad de los datos y privacidad de la información definidas por los usuarios y los administradores de los sistemas, con una actitud responsable.

IV. EVIDENCIA (S) DE DESEMPEÑO

Elabora un reporte final de un caso de estudio en donde se realice un monitoreo del status del actual de la red y se apliquen los mecanismos de seguridad para proteger dicha red, el cual deberá exponerse de forma oral y por escrito.

V. DESARROLLO POR UNIDADES

Competencia:

Analizar la importancia de la privacidad de la información en las redes de cómputo para ser más consiente del entorno y de la información que generan las organizaciones para garantizar el impacto de la seguridad como el siguiente desafío de la tecnología de las redes con una actitud crítica y responsable.

Contenido **Duración 4 hrs.**

1. La necesidad de protección

1.1. Motivación
1.2. ¿Cuál puede ser el valor de los datos?
1.3. Definiciones
1.4. Seguridad global
1.5. Impacto en la organización
1.6. Repaso de interconexión de redes (internetworking)

Competencia:

Aplicar los conceptos generales de la seguridad analizando los diferentes tipos de ataques, amenazas, vulnerabilidades y niveles de trabajo mediante los diferentes mecanismos y estándares para comprender la dimensión de la problemática y las posibles soluciones y proteger la información de las organizaciones con una actitud crítica y responsable.

Contenido **Duración 4 hrs.**

2. Conceptos Generales de seguridad

- 2.1. Principios fundamentales
- 2.2. Ataques, servicios y mecanismos
- 2.3. Ataques de seguridad (activos, pasivos)
- 2.4. Virus, gusanos y caballos de troya
- 2.5. Modelo multiniveles de seguridad
- 2.6. Análisis de riesgos
  - 2.6.1. Amenazas y vulnerabilidades
  - 2.6.2. Modelos de análisis de riesgos
- 2.7. Estándares de Internet y RFCs
- 2.8. Niveles de trabajo
  - 2.8.1. Confidencialidad
  - 2.8.2. Integridad
  - 2.8.3. Autenticidad
  - 2.8.4. No-repudio
  - 2.8.5. Disponibilidad de los recursos de la información
  - 2.8.6. Consistencia
  - 2.8.7. Control de acceso a los recursos
  - 2.8.8. Auditoría

Competencia:
Aplicar los conceptos del lado humano de la seguridad para que los usuarios, programadores y administradores de la red protejan la información en las organizaciones analizando y aplicando las políticas, normas y procedimientos así como los aspectos jurídicos y éticos con una actitud crítica y responsable.

Contenido **Duración 2 hrs.**

3. El lado humano de la seguridad
- 3.1. Políticas, normas y procedimientos
- 3.2. Programas de educación
- 3.3. Aspectos jurídicos y éticos

Competencia:
Aplicar los diferentes mecanismos de confidencialidad e integridad de la información mediante el análisis de los diferentes algoritmos para el cifrado de la información y de las tecnologías emergentes para la protección de la información y la infraestructura de cómputo de las organizaciones con una actitud crítica y responsable.

Contenido **Duración 4 hrs.**

4. Confidencialidad e integridad de la información
- 4.1. Criptografía
  - 4.1.1. Características de la criptografía
- 4.2. Cifrado y autentificación
  - 4.2.1. Algoritmos de llave privada
  - 4.2.2. Algoritmos de llave pública
  - 4.2.3. Infraestructura de llave pública (PKI)
- 4.3. Firmas digitales
- 4.4. Certificados
- 4.5. Autoridades de certificación
- 4.6. Aplicaciones criptográficas
  - 4.6.1. PGP, SSL, SSH, S/MIME
  - 4.6.2. VPNs & IPSec
- 4.7. Secure Socket Layer (SSL)
  - 4.7.1. SSL handshake

Competencia:

Aplicar los conceptos fundamentales de seguridad en cómputo protegiendo la información mediante el empleo de herramientas especializadas en los niveles de red (perimetral), sistemas operativos (nivel de host), aplicaciones (sistemas/programas) para garantizar la seguridad de las organizaciones con una actitud ética y responsable.

Contenido **Duración 6 hrs.**

5. Fortalecimiento de sistemas

- 5.1. Seguridad perimetral
  - 5.1.1. Firewalls
  - 5.1.2. Proxies
- 5.2. Seguridad en sistemas operativos
- 5.3. Seguridad en aplicaciones
- 5.4. Detectores de intrusos
- 5.5. Respuesta a incidentes
- 5.6. Análisis de estándares y guías
  - 5.6.1. Orange book
  - 5.6.2. Common criteria
  - 5.6.3. BS 7799

Competencia:
Identificar los diferentes ataques y vulnerabilidades mediante la toma de medidas preventivas y correctivas a través de la comprensión de los diferentes mecanismos existentes que utilizan los delincuentes informáticos para atacar y vulnerar sistemas con una actitud ética y responsable.

Contenido **Duración 6 hrs.**

6. Tipos de ataques y vulnerabilidades

- 6.1. Contraseñas
- 6.2. Email bombing & spamming
- 6.3. Problemas de seguridad en FTP
- 6.4. Problemas de seguridad en WWW
- 6.5. TFTP
- 6.6. Telnet
- 6.7. Los commandos “r”
- 6.8. Seguridad en NetBios
- 6.9. Negación de servicio (DOS)

Competencia:
Aplicar las diferentes herramientas de seguridad de uso libre existentes mediante la utilización de cada una de ellas en casos prácticos para la protección de la información de la organización con una actitud crítica y responsable.

Contenido **Duración 6 hrs.**

7. Herramientas de seguridad

- 7.1. Herramientas de control y seguimiento de accesos:
  - 7.1.1. tcp-wrappers, Netlog, Argus, tcpdump, Satan, ISS, Courtney, Gabriel, tcplist, nocol.
- 7.2. Integridad del sistema
  - 7.2.1. Cops, tiger, crack, tripwire, chkwtmp, chklastlog, spar, lsof, cpm, ifstatus, osh,noshell, trinux.

VI. ESTRUCTURA DE LAS PRÁCTICAS				
No. de Práctica	**Competencia(s)**	**Descripción**	**Material de Apoyo**	**Duración**
1	Instalar un sistema operativo de manera segura protegiendo los servicios y puertos de entradas utilizando las herramientas disponibles que brinde el sistema operativo en cuestión con una actitud ética y responsable.	Se instalará y se configurará el sistema operativo (windows/linux) dependiendo del uso que se le vaya a dar a la computadora (desarrollo, desktop, servidor,..). Una vez instalado el sistema operativo verificar los servicios/puertos habilitados utilizando herramientas como netstat, aports, etc. Deshabilitando aquellos servicios que no se utilicen o que no necesiten ser accedidos remotamente. También se le enseñara a elegir el esquema de contraseñas que mejor convenga para el tipo de instalación.	Computadora con sistema operativo Linux/windows . Netstat Aports	4 hrs. (HL)
2	Aplicar mecanismos de seguridad de intercambio de correo electrónico para proteger la información del cliente utilizando llaves públicas de uso libre tales como GnuPG o OpenPGP, con una actitud ética y responsable.	Se generarán llaves públicas para el intercambio de e-mail utilizando GnuPG u OpenPGP en conjunto con un cliente de email (e.g. Kmail) Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux . Utilerias: GnuPG Kmail Kgpg	4 hrs. (HL)

3	Generar códigos de seguridad de conexiones SSH (secure shell) para el intercambio de información utilizando canales seguros con una actitud ética y responsable.	Generación de llaves públicas de host utilizando SSH para el intercambio de comandos remotos a través de canales seguros e incluso para hacer conexiones remotas sin la necesidad de mandar el password por la red. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux. Utilería: OpenSSH	4 hrs. (HL)
4	Instalar y configurar conexiones seguras para proteger el intercambio de información utilizando protocolos de redes privadas virtuales (VPN) con una actitud ética y responsable.	Instalacion y configuracion de Infraestructura con VPNs utilizando FreeS/WAN (IPsec & IKE) u OpenVPN (SSL/TLS). Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux IPSec/ IKE	4 hrs. (HL)
5	Configurar un Firewall/Router para proteger la información de la red utilizando herramientas de software tales como IPtables, Routed o Zebra con una actitud ética y responsable.	Configuración de un Firewall/Router utilizando IPtables, Routed o Zebra. (Zebra tiene una interfaz de configuración igual que Cisco) Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux. IPTables/ Zebra	4 hrs. (HL)
6	Aplicar herramientas de seguridad para la detección de intrusos y encontrar patrones irregulares en la red utilizando aplicaciones tales como Snort o Prelud con una actitud ética y responsable.	Utilización de herramientas de seguridas para la detección de intrusos a nivel red utilizando herramientas como Snort o Prelude. Instalación, configuración y ejecución de Snort para encontrar patrones irregulares en el tráfico de red, tal como exploits, virus, entre otras.	Computadora con sistema operativo Linux. Snort	4 hrs. (HL)

		Se entregará un reporte escrito con los resultados y conclusiones		
7	Aplicar herramientas de seguridad para la detección de intrusos a nivel de hosts utilizando aplicaciones tales como Tripwire con una actitud ética y responsable.	Detección de intrusos a nivel de host utilizando la herramienta Tripwire. Instalación, configuración y ejecución de Tripwire creando una imagen de firmas digitales del sistema de archivos para detectar cambios en el mismo. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux	4 hrs. (HL)
8	Instalar, configurar y ejecutar herramientas de auditoria de sistemas para detectar anormalidades en la red utilizando una aplicación abierta conocida como Nessus con una actitud ética y responsable.	Auditoria a sistemas empleando la herramienta Nessus. Instalación, configuración y ejecución de Nessus para encontrar vulnerabilidades existentes en sistemas de diferentes plataformas. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux	4 hrs. (HL)
9	Instalar, configurar y ejecutar de herramientas para analizar protocolos en una red para auditar tráfico utilizando aplicaciones como Tcpdump y Wireshark con una actitud ética y responsable.	Auditoria a tráfico de red utilizando Tcpdump y Wireshark. Instalación, configuración y ejecución de tcpdump para auditar tráfico de red utilizando comandos en línea. Instalación, configuración y ejecución de Ethereal utilizando ambiente gráfico.	Computadora con sistema operativo Linux. Ethereal tcpdump	4 hrs. (HL)

		Se entregará un reporte escrito con los resultados y conclusiones		
10	Aplicar herramientas de monitoreo de tráfico de red para el reconocimiento de patrones utilizando la aplicación Ntop con una actitud ética y responsable.	Monitorear de tráfico de red utilizando una herramienta Ntop para conocer el patrón que forma el tráfico de la red. Hacer un análisis de tráfico de la red. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux. Ntop	4 hrs. (HL)
11	Instalar, configurar y ejecutar herramientas de seguridad de control de acceso a servicios de red para controlar su entrada a la red utilizando la herramienta TCPwrapper con una actitud ética y responsable.	Control de acceso a servicios de red utilizando la herramienta TCPWrappers Hacer un análisis de acceso a servicios Instalación, configuración y ejecución de TCPwrapper para controlar la entrada a servicios de red que ofrece un servidor.	Computadora con sistema operativo Linux. TCPwrapper	8 hrs. (HL)

VII. METODOLOGÍA DE TRABAJO

Investigación

La investigación será empleada en los trabajos extraclase que el docente pedirá al estudiante sobre temas de actualidad o sobre temas que se verán posteriormente en clase. El propósito de estos trabajos es que el estudiante aprenda hacer investigación en medios electrónicos (Internet), libros, y revistas sobre temas del área. Las fuentes serán tanto en el idioma inglés como español para fomentar la enseñanza del idioma extranjero. Los reportes deberán contener las referencias que se utilizaron para la realización del trabajo y debe contar imprescindiblemente una conclusión personal acerca de la investigación. El maestro debe enfatizar a los estudiantes que los reportes escritos sean claros y bien redactados, recalcándoles también las faltas de ortografía.

Exposición oral

El alumno debe ser capaz de desenvolverse oralmente al exponer un tema o al establecer una discusión sobre una temática en particular de la unidad de aprendizaje. El maestro debe involucrar a los estudiantes en la exposición oral ya sea de una noticia reciente o de un tema particular el alumno haya tenido el tiempo necesario para investigarlo.

Prácticas de Laboratorio

Llevar a la práctica los conocimientos teóricos vistos en clase es el mejor método de enseñanza-aprendizaje, por eso es importante que el estudiante desarrolle habilidades que le permitan resolver problemas reales en el área de telecomunicaciones y redes.

Exámenes de conocimientos

El maestro deberá aplicar al menos 2 exámenes de conocimientos durante el curso, de tal manera que refuercen los conocimientos aprendidos durante la clase. Los exámenes podrán ser de varios tipos, tales como: de preguntas abiertas, opción múltiple, crucigramas o mapas mentales.

Proyecto final

El maestro les asignará un proyecto final de un caso de estudio en donde se realice un monitoreo del status del actual de la red y se apliquen los mecanismos de seguridad para proteger dicha red, el cual deberá exponerse de forma oral y por escrito.

VIII. CRITERIOS DE EVALUACIÓN

Para la acreditación de la unidad de aprendizaje se atenderá al Estatuto Escolar Vigente, artículos 70-71, por lo que el estudiante deberá contar un mínimo de 80% de asistencias en el periodo. Tener un mínimo aprobatorio de 60 en su calificación final.

La evaluación general de la unidad de aprendizaje consistirá de exámenes teóricos, tareas-reportes, prácticas de laboratorio y una exposición oral con un reporte escrito.

Los porcentajes de evaluación serán los siguientes:

Exámenes	40%
Tareas/prácticas	30%
Proyecto final	30%
Total	100%

Criterio de acreditación

- Resolver al menos 2 exámenes parciales en tiempo y forma.
- Las tareas y las prácticas serán estrictamente individuales
- Deberán ser al menos 10 prácticas y tareas extraclase por semestre
- Cumplir con las prácticas y tareas extraclase en tiempo y forma.
- Cumplir con el proyecto final, su presentación oral y reporte escrito en tiempo y forma.

Criterio de evaluación

- Las tareas, prácticas y exámenes serán resueltos en clase posterior de la entrega para que el estudiante conozca inmediatamente la solución propuesta en cada uno de los trabajos o exámenes.
- En el caso de la exposición final por equipo, la evaluación se dividirá en dos: reporte escrito y exposición, en el primer caso la calificación será por equipo y los puntos a evaluar serán, contenido, claridad y forma, así como ortografía y redacción; para la exposición oral ésta se calificará de manera individual y los puntos a evaluar serán, dominio del tema, claridad y estructura. Los alumnos puede ayudarse en la exposición mediante apoyos visuales tales como proyector de transparencias, acetatos u medios multimedia.
- El proyecto final será por equipos y constará de la aplicación funcionando, un reporte escrito y la exposición oral. La exposición oral se evaluara individualmente, el reporte escrito y la aplicación funcionando se calificará por equipo.

IX. BIBLIOGRAFÍA

Básica	Complementaria
Castellanos , Luis R. (2015). Seguridad en Informática. Ed. Académica Española , Herzog, P., Jordan, M. B., Monroe, B., & Norman, G. (2015). *The Network Security Essentials: Study Guide & Workbook-Volume 1*. ISECOM. Kizza, J. M. (2015). *Guide to computer network security*. Springer. Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing*. Prentice Hall Professional Technical Reference.	Matt, B. (2005). Computer security e art and science. *003-02-14)[2009-05-23]. http://www, amazon, corn/Computer-Security-Science-Matt-Bishop/dp/0201440997*. [Clásico] Smith, R. E. (2015). *Elementary information security*. Jones & Bartlett Publishers. Stewart, J. M. (2014). *CompTIA Security+ Review Guide: Exam SY0-401*. John Wiley & Sons. Wells, N. (2000). *Guide to Linux Networking and Security*. Course Technology Press. Home Network Security https://www.cert.org/information-for/home_networks.cfm Network Security Resources https://www.sans.org/network-security/

X. PERFIL DOCENTE

Profesionista en cómputo o áreas afines con experiencia docente y conocimientos de redes de comunicaciones, el dominio de sistemas operativos tipo GNU Linux, Windows, Apple iOS, así como del dominio de herramientas de cómputo emergentes para proteger un sistema de cómputo ante vulnerabilidades. Se requiera de un docente con enfoque ético, para que estas herramientas tengan un uso responsable.