UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

COORDINACIÓN GENERAL DE FORMACIÓN PROFESIONAL

PROGRAMA DE UNIDAD DE APRENDIZAJE

I. DATOS DE IDENTIFICACIÓN

1. Unidad Académica: Facultad de Ingeniería, Arquitectura y Diseño, Ensenada; Facultad Ciencias Químicas e Ingeniería, Tijuana; y Facultad de Ciencias de la Ingeniería y Tecnología, Valle de las Palmas

2. Programa Educativo: Ingeniero en Software y Tecnologías Emergentes

3. Plan de Estudios: 2022-1

4. Nombre de la Unidad de Aprendizaje: Seguridad del Software

5. Clave: 40022

6. HC: 02 **HT:** 00 **HL:** 02 **HPC:** 00 **HCL:** 00 **HE:** 02 **CR:** 06

7. Etapa de Formación a la que Pertenece: Terminal

8. Carácter de la Unidad de Aprendizaje: Obligatoria

9. Requisitos para Cursar la Unidad de Aprendizaje: Ninguno

Equipo de diseño de PUA
Carlos Francisco Álvarez Salgado
Eduardo Ceseña Beltrán

Vo.Bo. de subdirector(es) de Unidad(es) Académica(s)
Humberto Cervantes De Ávila
Daniela Mercedes Martínez Platas
Noemí Hernández Hernández

Fecha: 23 de febrero de 2021

II. PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

El aseguramiento en la disponibilidad de las comunicaciones, la integridad de los datos y la privacidad de la información es la prioridad en la infraestructura de cómputo. Los temas expuestos y desarrollados en esta asignatura, deberán de proveer las herramientas para que los alumnos puedan diseñar e implementar infraestructura de servicios que funcione apropiadamente utilizando las mejores prácticas. Esta asignatura es de carácter obligatoria de la etapa terminal y contribuye al área de conocimiento Infraestructura de Sistemas

III. COMPETENCIA GENERAL DE LA UNIDAD DE APRENDIZAJE

Analizar y documentar las amenazas potenciales a un sistema informático, mediante patrones para la seguridad, para mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada en entornos informáticos, de manera organizada y metódica, con una actitud de colaboración y honestidad.

IV. EVIDENCIA(S) DE APRENDIZAJE

Portafolio de casos relacionados con la seguridad en entornos informáticos, describiendo el tipo de amenaza y los patrones para la seguridad a los que corresponde, junto con las soluciones propuestas.

V. DESARROLLO POR UNIDADES
UNIDAD I. Fundamentos de seguridad

Competencia:
Analizar los fundamentos de seguridad a partir de los conceptos de seguridad y la naturaleza de las amenazas para determinar la importancia de la protección de los recursos informáticos, de comunicación y almacenaje, con pensamiento crítico.

Contenido: **Duración:** 4 horas

1.1. Conceptos de aseguramiento de la información
1.2. Naturaleza de las amenazas

UNIDAD II. Cifrado

Competencia:
Determinar el funcionamiento de los mecanismos de cifrado a partir de teoría de cifrado y su práctica para proteger información, con responsabilidad.

Contenido: **Duración:** 4 horas

2.1. Cifrado
2.2. Firmas digitales
2.3. Funciones hash

UNIDAD III. Criptografía

Competencia:
Explorar el uso del cifrado en la infraestructura de cómputo para proteger datos y la comunicación, mediante la criptografía, con actitud analítica y objetiva.

Contenido: **Duración:** 4 horas

3.1. Protocolos comunes
3.2. Aplicaciones
3.3. Fortalezas y debilidades

UNIDAD IV. Seguridad informática y de red

Competencia:
Describir los problemas que presentan la infraestructura de red, mediante soluciones como la implementación de una infraestructura de llave publica, cortafuegos y los detectores de intruso, para salvaguardar la seguridad y la privacidad de los datos, con actitud analítica.

Contenido: **Duración:** 10 horas

4.1. Amenazas y ataques a la seguridad en red
4.2. Criptografía para seguridad en red
4.3. Mecanismos y herramientas de protección y defensa

UNIDAD V. Patrones para la seguridad

Competencia:
Implementar buenas prácticas con distintas tecnologías de infraestructura informática, para asegurar la calidad de los servicios, la confidencialidad y privacidad de la información, con respeto y eficiencia.

Contenido: **Duración:** 10 horas

5.1. Patrones para la seguridad en los sistemas operativos
5.2. Patrones para la seguridad en red
5.3. Patrones para la seguridad en los servicios Web
5.4. Patrones para la seguridad en Middleware

VI. ESTRUCTURA DE LAS PRÁCTICAS DE LABORATORIO				
No.	**Nombre de la Práctica**	**Procedimiento**	**Recursos de Apoyo**	**Duración**
UNIDAD II				
1	**Cifrado simétrico**	1. Seguir un algoritmo. 2. Implementar una aplicación con base en un algoritmo. 3. Utilizar la aplicación para cifrar un conjunto de datos. 4. Descifrar conjuntos de datos a través de la aplicación. 5. Documentar la práctica. 6. Entregar la práctica al profesor para retroalimentación.	• Computadora con internet. • Página de cifrado: https://gchq.github.io/CyberChef/	3 horas
2	**Cifrado asimétrico**	1. Seleccionar una herramienta para crear una llave pública y privada. 2. Intercambiar las llaves públicas con otros alumnos y el maestro. 3. Intercambiar mensajes codificados a través de las llaves con otros alumnos 4. Decodificar los mensajes recibidos con la llave y herramientas especializadas. 5. Documentar la práctica. 6. Entregar la práctica al profesor para retroalimentación.	• Computadora con internet. • Software de acceso libre.	3horas
3	**Detector de intrusos a nivel de Host**	1. Definir los objetos a inspeccionar en un sistema de archivos. 2. Configurar la herramienta para utilizar el análisis de firmas digitales. 3. Generar una base de datos	• Computadora con internet. • Software de acceso libre.	3 horas

		con las firmas digitales de los objetos que se están inspeccionando. 4. Realizar cambios en el sistema de archivos, preferentemente en carpetas controladas (se sugiere que el maestro realice esta acción). 5. Realizar una corrida con la herramienta para demostrar el cambio de archivo con las firmas digitales. 6. Documentar la práctica. 7. Entregar la práctica al profesor para retroalimentación.		
UNIDAD III				
4	**Certificados digitales**	1. Elegir una herramienta para crear certificados digitales. 2. Definir los datos que integrarán certificados digitales. 3. Ejecutar la herramienta. 4. Ingresar los datos solicitados durante la ejecución de la herramienta. 5. Validar los certificados con la misma herramienta. 6. Documentar la práctica. 7. Entregar la práctica al profesor para retroalimentación.	• Computadora con internet. • Software de acceso libre.	3 horas
5	**PKI**	1. Definir una autoridad certificadora. 2. Generar certificados usados por personas y servicios utilizando la autoridad certificadora. 3. Documentar la práctica. 4. Entregar la práctica al profesor	• Computadora con internet. • Software de acceso libre.	3 horas

		para retroalimentación.		
6	**VPN**	1. Utilizar un sistema operativo que ofrezca VPN. 2. Interconectar dos nodos VPN realizando un puente. 3. Comprobar la comunicación de las redes privadas detrás de cada nodo. 4. Documentar la práctica. 5. Entregar la práctica al profesor para retroalimentación.	• Computadora con internet. • Software de acceso libre.	3 horas
UNIDAD IV				
7	**Implementación de un servidor web con soporte SSL**	1. Instalar un servicio web 2. Utilizar una herramienta para generar un certificado SSL para su servicio web. 3. Configurar el servicio web para que utilice el certificado. 4. Demostrar que el sitio web utilice el certificado a través de un navegador web. 5. Documentar la práctica. 6. Entregar la práctica al profesor para retroalimentación.	• Computadora con internet. • Software de acceso libre.	3 horas
8	**Aplicar un cortafuegos en una máquina local**	1. Implementar las políticas que define el profesor. 2. Demostrar la funcionalidad de las políticas. 3. Documentar la práctica. 4. Entregar la práctica al profesor para retroalimentación.	• Computadora con internet. • Software de acceso libre.	3 horas
9	**Detectores de intruso a nivel de red**	1. Implementar un detector de intrusos haciendo uso de un sistema operativo que ya lo tenga incluido. 2. Monitorear el tráfico de red con	• Computadora con internet. • Software de acceso libre.	4 horas

		el detector de intruso. 3. Encontrar los problemas que el profesor ocasiones en el tráfico con el detector de intrusos. 4. Documentar la práctica. 5. Entregar la práctica al profesor para retroalimentación.		
UNIDAD V				
10	**Escaneo de vulnerabilidades con software especializado**	1. Utilizando un software especializado realizar un escaneo de puertos a dispositivos que el profesor señale. 2. Realizar un reporte del análisis de escaneo de puerto haciendo notar las generalidad o problemas detectados. 3. Documentar la práctica. 4. Entregar la práctica al profesor para retroalimentación.	• Computadora con internet. • Software de acceso libre.	2 horas
11	**Mitigación de ataques de fuerza bruta y escaneo de puertos**	1. Instalar una aplicación que analice bitácora para detectar un intento de inicio de sesión fallido. 2. Realizar con otra terminal intentos fallidos de sesión para obtener datos. 3. Instalar una aplicación para detectar el escaneo puertos 4. Realizar el escaneo de puertos en el equipo. 5. Documentar la práctica. 6. Entregar la práctica al profesor para retroalimentación.	• Computadora con internet. • Software de acceso libre.	2 horas

VII. MÉTODO DE TRABAJO

Encuadre: El primer día de clase el docente debe establecer la forma de trabajo, criterios de evaluación, calidad de los trabajos académicos, derechos y obligaciones docente-alumno.

Estrategia de enseñanza (docente):

- Técnica expositiva
- Instrucción guiada
- Estudio de casos
- Solución de problemas

Estrategia de aprendizaje (alumno):

- Trabajo colaborativo
- Investigación documental
- Ejercicios prácticos
- Exposición

VIII. CRITERIOS DE EVALUACIÓN

La evaluación será llevada a cabo de forma permanente durante el desarrollo de la unidad de aprendizaje de la siguiente manera:

Criterios de acreditación

- Para tener derecho a examen ordinario y extraordinario, el estudiante debe cumplir con los porcentajes de asistencia que establece el Estatuto Escolar vigente.
- Calificación en escala del 0 al 100, con un mínimo aprobatorio de 60.

Criterios de evaluación

- Evaluaciones parciales……30%
- Prácticas de laboratorio…….. 50%
- Tareas……... 15%
- Portafolio de evidencias…….… 05%

Total…….100%

IX. REFERENCIAS

Básicas

Andress, J. (2019). *Foundations of information security*. Estados Unidos: No Starch Press.

Aumasson, J. P. (2017). *Serious Cryptography*. Estados Unidos: No Starch Press.

Fernandez-Buglioni, E. (2013). *Security patterns in practice.* Reino Unido: Wiley. [Clásica].

Helfrich, J. (2019). *Security for software engineers*. Estados Unidos: CRC Press.

Complementarias

Brotherston, L. y Berlin, A. (2017). *Defensive security handbook*. Estados Unidos: O´Reilly.

Dark, M., Harter, N., Morales, L. y Garcia, M. A. (Junio, 2008). An information security ethics education model. Journal of *Computing Sciences in Colleges, 23* (6). Recuperado de https://dl.acm.org/doi/10.5555/1352383.1352399

Forshaw, J. (2017). *Attacking network protocols*. Estados Unidos: No Starch Press.

Schneier, B. (2015). *Applied cryptography*. Estados Unidos: Wiley.

Wysopal, C, Nelson, L., Zovi, D. D. y Dustin, E. (2007). The art of software security testing. Estados Unidos: Addison-Wesley. [Clásica].

X. PERFIL DEL DOCENTE

El docente que imparta la unidad de aprendizaje Seguridad en Entornos Informáticos debe contar con título de Ingeniero en Computación o área afín, con conocimientos de sistemas operativos, redes de computadoras y seguridad de la información; preferentemente con estudios de posgrado en ciencias de la computación y al menos dos años de experiencia en el área de seguridad informática y docencia.