UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

COORDINACIÓN GENERAL DE FORMACIÓN PROFESIONAL

PROGRAMA DE UNIDAD DE APRENDIZAJE

I. DATOS DE IDENTIFICACIÓN

1. **Unidad Académica**: : Facultad de Ciencias Administrativas y Sociales, Ensenada; Facultad de Ciencias Administrativas, Mexicali; Facultad de Ciencias de la Ingeniería, Administrativas y Sociales, Tecate; y Facultad de Contaduría y Administración, Tijuana.

2. **Programa Educativo:** Licenciado en Inteligencia de Negocios

3. **Plan de Estudios:** 2021-2

4. **Nombre de la Unidad de Aprendizaje:** Seguridad Informática

5. **Clave**: 39050

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

7. **Etapa de Formación a la que Pertenece**: Disciplinaria

8. **Carácter de la Unidad de Aprendizaje**: Obligatoria

9. **Requisitos para cursar la Unidad de Aprendizaje:** Ninguno

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
REGISTRADO
21 MAYO 2021
REGISTRADO
COORDINACIÓN GENERAL DE FORMACIÓN PROFESIONAL

Equipo de diseño de PUA	**Firma**	**Vo.Bo. de subdirector(es) de Unidad(es) Académica(s)**	**Firma**
Guillermo Alberto Loam Gómez		Adelaida Figueroa Villanueva	
Javier Fermín Padilla Sánchez		Angélica Reyes Mendoza	
Esteban Pérez Flores.		Esperanza Manrique Rojas	
Ricardo Ching Wesman.		Jesús Antonio Padilla Sánchez	

Fecha: 12 de marzo de 2020

II. PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Esta unidad de aprendizaje proporciona los fundamentos, herramientas y riesgos de seguridad informática, así como la metodología de implementación de un plan de seguridad para salvaguardar los activos informáticos de una organización.

Se ubica en la etapa disciplinaria, es de carácter obligatoria y forma parte del área de conocimiento de Infraestructura de Tecnologías de Información

III. COMPETENCIA GENERAL DE LA UNIDAD DE APRENDIZAJE

Proponer un marco de seguridad apropiado basado en las normas y estándares nacionales e internacionales de seguridad informática pertinentes para mantener la confiabilidad, integridad y disponibilidad de la información y la infraestructura tecnológica con profesionalismo, ética y honestidad.

IV. EVIDENCIA(S) DE APRENDIZAJE

Elaborar propuesta de plan de seguridad para una organización, basado en metodologías, normativa, estándares y el análisis de la infraestructura, para mejorar la integridad de la información y los procesos que se requieren para garantizar y salvaguardar la integridad de sus activos informáticos.

V. DESARROLLO POR UNIDADES
UNIDAD I. Fundamentos de seguridad Informática

Competencia:
Identificar los fundamentos, pilares y estándares de seguridad, mediante la revisión de sus características, para conocer el ámbito de la seguridad informática, con actitud reflexiva, crítica, y objetiva.

Contenido: **Duración:** 4 horas

1.1 Definiciones y Conceptos básicos
1.2 Pilares de la seguridad informática
    1.2.1 Confidencialidad
    1.2.2 Integridad
    1.2.3 Disponibilidad
    1.2.4 Autenticación
1.3 Estándares de seguridad
    1.2.1 COBIT
    1.2.2 ITIL
    1.2.3 ISO IEC27000, ISO /IEC 20000, ISO 38500

UNIDAD II. Tipos de seguridad informática

Competencia:
Analizar los diferentes tipos de seguridad informática, para comprender las ventajas, utilidad e importancia de su aplicación en las organizaciones, mediante el estudio de las técnicas y esquemas particulares de cada uno de ellos, con actitud analítica, responsable y honesta.

Contenido: **Duración:** 4 horas

2.1 Seguridad en hardware
2.2 Seguridad en software
2.3 Seguridad en redes

UNIDAD III. Privacidad y protección de los datos

Competencia:
Examinar el impacto de la privacidad y protección de los datos en una organización, para resguardar la seguridad informática, mediante el análisis de los métodos de ataque, protección de datos y sus protocolos de seguridad con objetividad, actitud analítica y ética.

Contenido: **Duración:** 6 horas

3.1 Métodos de ataque
3.2 Mecanismos de protección
3.3 Criptografía
3.4 Cifrado simétrico y asimétrico
3.5 Protocolos de seguridad

UNIDAD IV. Herramientas de seguridad informática

Competencia:
Emplear distintas herramientas de seguridad informática, para conocer las ventajas y desventajas de su implementación , mediante la comparación de sus características y requerimientos, con actitud organizada, proactiva y responsable.

Contenido: **Duración:** 6 horas

4.1 Software de respaldo y recuperación de información
4.2 Herramientas antivirus, antimalware
4.3 Cortafuegos
4.4 Seguridad física para acceso y protección de las instalaciones
4.5 Software de escaneo de vulnerabilidades

UNIDAD V. Riesgos de seguridad

Competencia:
Crear planes de contingencia y recuperación, para evaluar y mitigar los riesgos de seguridad informática que se pueden presentar en una organización, mediante técnicas de análisis y administración de los mismos, de manera profesional, analítica y responsable.

Contenido: **Duración:** 6 horas

5.1 Análisis de riesgos
5.2 Administración de riesgos
5.3 Planes de contingencia y recuperación

UNIDAD VI. Plan de seguridad

Competencia:
Elaborar un plan de seguridad informática, para salvaguardar la confidencialidad, integridad y disponibilidad de los activos informáticos de una organización mediante la aplicación de la metodología de seguridad informática, con profesionalismo, actitud colaborativa y responsabilidad.

Contenido: **Duración:** 6 horas

- 6.1 Auditoría de seguridad
- 6.2 Elementos Básicos de un plan de seguridad
  - 6.2.1 Alcance del Plan de Seguridad
  - 6.2.2 Caracterización de la Infraestructura tecnológica
  - 6.2.3 Políticas de seguridad
  - 6.2.4 Procedimientos de Seguridad
    - 6.2.4.1 Medidas Físicas
    - 6.2.4.2 Medidas Lógicas
- 6.3 Desarrollo del Plan de Seguridad
- 6.4 Implementación

VI. ESTRUCTURA DE LAS PRÁCTICAS DE TALLER				
No.	**Nombre de la Práctica**	**Procedimiento**	**Recursos de Apoyo**	**Duración**
UNIDAD III				
1	Métodos de ataque y protección	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga acerca de los principales mecanismos de ataque y protección 3. Elabora una representación gráfica utilizando herramientas digitales. 4. Presenta su representación gráfica .	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	2 horas
2	Criptografía, cifrado simétrico y asimétrico	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga acerca de los temas correspondientes 3. Identifica las características y elementos de cada uno de ellos. 4. Realiza una representación gráfica utilizando herramientas digitales. 5. Presenta su representación gráfica .	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	2 horas
3	Protocolos de seguridad	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga acerca de los diferentes protocolos de seguridad, sus características y elementos 3. Realiza una representación gráfica utilizando herramientas	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	2 horas

		digitales. 4. Presenta su representación gráfica .		
UNIDAD IV				
4	Herramientas antivirus, antimalware	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga software de antivirus y antimalware que existen en la actualidad 3. Selecciona un software de open source o de prueba e Instalalo en una computadora. 4. Realiza pruebas de detección de virus o malware 5. Haz una representación gráfica con los resultados obtenidos.	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	2 horas
5	Cortafuegos	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga software para cortafuegos 3. Selecciona un software de open source o de prueba e Instalalo en una computadora. 4. Realiza pruebas de protección y detección. 5. Haz una representación gráfica con los resultados obtenidos.	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	3 horas
6	Informática forense	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga software de análisis y búsqueda de información en un disco duro 3. Selecciona un software de open	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	3 horas

		source o de prueba e Instalalo en una computadora. 4. Realiza pruebas en un disco duro de búsqueda de información perdida o borrada 5. Haz una representación gráfica con los resultados obtenidos.		
7	Software de escaneo de vulnerabilidades	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga qué software de escaneo de vulnerabilidades existen en la actualidad. 3. Selecciona un software open source e instalalo en una computadora 4. Realiza pruebas en la red 5. Presenta su representación gráfica los resultados de la prueba.	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	3 horas
8	Sistema de detección de intrusos	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga qué software de detección de intrusos existen en la actualidad. 3. Selecciona un software open source e instalalo en una computadora 4. Realiza pruebas en la red 5. Presenta su representación gráfica los resultados de la prueba.	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	3 horas
UNIDAD V				

9	Herramientas de análisis de riesgos.	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investigar software para evaluar riesgos y vulnerabilidades existentes en la actualidad. 3. Selecciona software para el análisis de riesgos. 4. Emplear software para evaluar riesgos y vulnerabilidades existentes en un sistema informático 5. Presenta reporte de análisis de riesgos.	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	4 horas
10	Plan de contingencia	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga acerca de los temas correspondientes 3. Identifica las características y elementos de cada uno de ellos. 4. Realiza un plan de contingencia y recuperación para una organización hipotética 5. Presenta su plan de recuperación al docente para retroalimentación	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	4 horas
UNIDAD VI				
11	Plan de seguridad informática	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga el formato y los elementos que debe contener un plan de seguridad informática. 3. La práctica consiste en	● Computadora. ● Internet. ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.).	4 horas

		desarrollar un plan de seguridad informática para una organización hipotética. 4. Una vez hecho el plan realiza una presentación grupal del mismo. 5. Se realizará posterior a la presentación una dinámica de grupo con cuestionamientos del plan presentado, por parte de los compañeros del grupo. 6. Se realizará un reporte con los resultados.		

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):

- Estudio de caso
- Método de proyectos
- Aprendizaje basado en problemas
- Técnica expositiva
- Ejercicios prácticos
- Selección y proyección de material audiovisual

Estrategia de aprendizaje (alumno):

- Investigación
- Estudio de caso
- Trabajo en equipo
- Exposiciones
- Prácticas de laboratorio
- Organizadores gráficos
- Resúmenes

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

- Tareas y participación……...…...15%
- Evaluaciones parciales……..…….. 20%
- Exposición……15%
- Prácticas de taller…..……... 20%
- Plan de seguridad ……..……..... 30%

Total……100%

IX. REFERENCIAS

Básicas

Caballero, D., y Cilleros M. (2019). *Ciberseguridad y transformación digita*l. España: Anaya Multimedia

Kamberg, M., y Jiménez, A. (2018). *Ciberseguridad: protege tu identidad y tus datos*. Estados Unidos: Rosen Central.

Mitnick, K. y Vamosi, R. (2018). *El arte de la invisibilidad*. México: Anaya.

Romero, M., Figueroa G., Vera D., Álava D., Parrales G., Álava C., Murillo A. y Castillo M. (2018). I*ntroducción a la seguridad informática y el análisis de vulnerabilidades*. España: Área de Innovación y Desarrollo,S.L.

Ventre, D. (2020). *Artificial Intelligence, Cybersecurity and Cyber Defence*. Wiley-ISTE

Complementarias

Banco Interamericano de Desarrollo, Organización de los Estados Americanos. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*.

Cisco.(2020).¿Qué es la ciberseguridad?. Recuperado de https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Norton, P. (2014). *Introducción a la computación* (6ª ed.). México: McGraw-Hil. [clásica]

Villarreal, S. (2007). *Introducción a la computación: Teoría y manejo de paquetes* (2ª ed.). México: McGraw-Hill. [clásica]

X. PERFIL DEL DOCENTE

El docente que imparte la unidad de aprendizaje debe contar con título de Licenciatura inteligencia de negocios, Licenciado en Informática. Ingeniero en computación o preferentemente con maestría en área afín. Contar experiencia mínima de tres años en la docencia y profesional en infraestructura tecnológica, ciberseguridad y redes de cómputo comprobable. Además, debe ser dedicado, organizado, que promueva la investigación, el trabajo en equipo y tener facilidad de palabra.