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:** Ciberseguridad para Negocios

5. **Clave**: 39074

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

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

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

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
Javier Fermín Padilla Sánchez
Sandra Julieta Saldivar González
Hernán Adrián Parra Galaviz

Vo.Bo. de subdirectores de las Unidades Académicas
Adelaida Figueroa Villanueva
Angélica Reyes Mendoza
Esperanza Manrique Rojas
Jesús Antonio Padilla Sánchez

Fecha: 12 de noviembre de 2020

II. PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Esta unidad de aprendizaje proporciona los fundamentos, normativas y estándares, así como la importancia de la ciberseguridad, lo que permite desarrollar un plan en las organizaciones, y así salvaguardar su infraestructura tecnológica.

Se ubica en la etapa disciplinaría, es de carácter optativa y forma parte del área de conocimiento de Infraestructura de Tecnologías de Información.

III. COMPETENCIA GENERAL DE LA UNIDAD DE APRENDIZAJE

Elaborar una propuesta de plan de ciberseguridad, basada en las herramientas metodológicas, normativa, estándares y el análisis de la infraestructura, para proponer las medidas más adecuadas en una organización, con responsabilidad y honestidad.

IV. EVIDENCIA(S) DE APRENDIZAJE

Plan de ciberseguridad en 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 el adecuado funcionamiento de la empresa, así como las recomendaciones necesarias para optimizar sus recursos e infraestructura tecnológica.

V. DESARROLLO POR UNIDADES
UNIDAD I. Fundamentos de ciberseguridad

Competencia:
Analizar los conceptos básicos de ciberseguridad**,** oficial de seguridad de la información, así como los organismos reguladores, mediante la revisión de sus especificaciones de parámetros, funciones, protocolos y normas, para familiarizarse en el ámbito de la seguridad informática, con actitud reflexiva, crítica, y objetiva.

Contenido: **Duración:** 4 horas

1.1. Conceptos básicos de ciberseguridad.
1.2. Oficial de seguridad de la Información (CIO).
1.3. Organismos nacionales e internacionales aplicables a la seguridad Cibernética

UNIDAD II. Normativas y estándares de ciberseguridad

Competencia:
Examinar normas, estándares y buenas prácticas**,** mediante la revisión de sus características, aplicación y enfoque, para determinar las directrices de seguridad en la organización, con actitud reflexiva, crítica, y objetiva.

Contenido: **Duración:** 5 horas

2.1. Normativas y estándares que regulan la seguridad cibernética
- 2.1.1. ISO/IEC 27001 y 27002
- 2.1.2. NERC
- 2.1.3. NIST
- 2.1.4. ISO 15408

UNIDAD III. Impacto social de la vulnerabilidad digital

Competencia:
Distinguir el panorama actual de la vulnerabilidad digital, a través del análisis de la evolución, riesgos y amenazas cibernéticas, además de la identificación de técnicas científicas y analíticas de la informática forense, para la preservación de la información y la mitigación de los riesgos, con actitud metódica, organizada y honesta.

Contenido: **Duración:** 5 horas

3.1. Evolución del cibercrimen, especialización delincuencial y nuevos delitos
    3.1.1. Ataque cibernético
    3.1.2. Tipos de ataques
3.2. Respuesta a incidentes.
3.3. Riesgos y amenazas del cibercrimen
3.4. Informática forense

UNIDAD IV. Importancia de la ciberseguridad en los negocios

Competencia:
Distinguir el panorama de la ciberseguridad en los negocios, a través del análisis del entorno actual, su cultura y tendencias, para reconocer la importancia de contar con un plan de protección de seguridad integral, con actitud proactiva, organizada y honesta.

Contenido: **Duración:** 8 horas

4.1. Ciberinteligencia
4.2. Ciberdefensa
4.3. Cultura de ciberseguridad.
4.4. Tendencias de ciberseguridad en los negocios

UNIDAD V. Infraestructura y plan de ciberseguridad en la empresa

Competencia:
Distinguir la seguridad en la infraestructura de red de una organización, para desarrollar un plan de seguridad cibernética, mediante normativas y estándares que permitan salvaguardar la integridad de la información, con creatividad, ética, responsabilidad.

Contenido: **Duración:** 10 horas

5.1. Seguridad en redes.
- 5.1.1. Políticas y normativas de la ciberseguridad
- 5.1.2. Resguardo y acceso de infraestructura
- 5.1.3. Métodos de seguridad de la información
- 5.1.4. Seguridad en dispositivos

5.2. Colaboración en materia de seguridad y justicia.

5.3 Caso práctico
- 5.3.1. Análisis de vulnerabilidad cibernética (Pentest)
- 5.3.2. Elementos de un plan o programa de ciberseguridad
- 5.3.3. Desarrollo del plan de ciberseguridad

VI. ESTRUCTURA DE LAS PRÁCTICAS DE TALLER				
No.	**Nombre de la Práctica**	**Procedimiento**	**Recursos de Apoyo**	**Duración**
UNIDAD III				
1	Evolución del cibercrimen	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga acerca de la evolución del cibercrimen. 3. Identifica los principales momentos del cibercrimen. 4. Realiza en representación gráfica la evolución de los cibercriminales. 5. Presenta su representación gráfica.	● Computadora ● Internet ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.)	2 horas
2	Ataques cibernéticos	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga acerca de la evolución de los ataques cibernéticos. 3. Identifica los principales ataques cibernéticos. 4. Realiza en representación gráfica la evolución ataques cibernéticos.	● Computadora ● Internet ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.)	2 horas
3	Respuesta de Riegos y amenazas del cibercrimen	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga acerca de los riesgos y amenazas del cibercrimen. 3. Identifica los riesgos y amenazas del cibercrimen. 4. Realiza en representación gráfica el nivel de riesgos y amenazas en una	● Computadora ● Internet ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.)	3 horas

		organización.		
4	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 source o de prueba e Instala en una computadora. 4. Realiza pruebas en un disco duro de búsqueda de información perdida o borrada. 5. Realiza representación gráfica con los resultados obtenidos.	● Computadora ● Internet ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.)	4 horas
UNIDAD IV				
5	Sistema de monitoreo de red	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga qué software de monitoreo de red existen en la actualidad. 3. Selecciona un software open source e instala en una computadora. 4. Realiza pruebas en la red. 5. Presenta representación gráfica los resultados de la prueba.	● Computadora ● Internet ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.)	4 horas
6	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 instala en una	● Computadora ● Internet ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.)	4 horas

		computadora 4. Realiza pruebas en la red 5. Presenta representación gráfica los resultados de la prueba.		
UNIDAD V				
7	Escaneo de vulnerabilidades internas	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga software para la detección de vulnerabilidades existentes en la actualidad. 3. Selecciona software Pentest e instala en una computadora. 4. Realiza pruebas de penetración e identifica vulnerabilidades internas. 5. Presenta reporte de vulnerabilidades internas identificadas.	● Computadora ● Internet ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.)	4 horas
8	Resguardo y recuperación de información	1. Atiende las orientaciones del profesor para elaborar la práctica. 2. Investiga los software o servicios en la nube que existen en la actualidad para resguardo y recuperar información. 3. Selecciona un software de open source y un servicio en la nube para realizar pruebas de resguardo y recuperación de información. 4. Realiza representación gráfica con los resultados obtenidos.	● Computadora ● Internet ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.)	4 horas

9	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 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.	● Computadora ● Internet ● Medio de proyección ● Recursos bibliográficos (libros, revistas, capítulos de libros, artículos, manuales, etc.)	5 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):

- 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 taller
- 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 ciberseguridad …….....….. 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 en inteligencia de negocios, Informática. 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.