

Benemérita Universidad Autónoma de Puebla

Vicerrectoría de Docencia

Dirección de Educación Superior

Facultad de Ciencias de la Computación



PLAN DE ESTUDIOS (PE): Licenciatura en Ingeniería en Ciencias de la Computación

ÁREA: Redes

ASIGNATURA: Ingeniería Social

CÓDIGO: ICCA 001

CRÉDITOS: 6



FECHA: 2 de julio de 2024

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Lil-o Mantilla Ne

Daniel M. Gonzalez Arriaga

Benemérita Universidad Autónoma de Puebla

Vicerrectoría de Docencia

Dirección de Educación Superior

Facultad de Ciencias de la Computación



1. DATOS GENERALES

Nivel Educativo:	Licenciatura
Nombre del Plan de Estudios:	Licenciatura en Ingeniería en Ciencias de la Computación
Modalidad:	Escolarizada
Modalidad de impartición de la Asignatura:	Presencial
Nombre de la Asignatura:	Ingeniería Social
Ubicación:	Básico
Correlación:	
Asignaturas Precedentes:	Ninguna
Asignaturas Consecuentes:	Matemáticas Discretas

2. CARGA HORARIA DEL ESTUDIANTE (Ver Malla)

Concepto	Horas por semana		Horas de trabajo independiente e por periodo	Total, de horas por periodo	Total, de créditos
	Teoría	Práctica			
Horas teoría, práctica y trabajo independiente (16 horas = 1 crédito)	3	2	0	90	6

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Lilia Mantilla Navarrete

Benemérita Universidad Autónoma de Puebla

Vicerrectoría de Docencia

Dirección de Educación Superior

Facultad de Ciencias de la Computación



3. REVISIONES Y ACTUALIZACIONES

Autores:	Adriana Hernández Beristain Abraham Maldonado García Ana Claudia Zenteno Vázquez Daniel Marcelo González Arriaga Elsa Chavira Martínez Erika Annabel Martínez Mirón Guillermina Sánchez Román Mariano Larios Gómez Miguel Ángel León Chávez
Fecha de diseño:	24 de junio de 2024
Fecha de la última actualización:	
Fecha de aprobación por parte de la academia de área, departamento u otro.	2 de julio de 2024
Revisores:	
Sinopsis de la revisión y/o actualización:	Considerando la propuesta: de la creación de la asignatura Ingeniería Social, por parte de la CDESC de la carrera Licenciatura en Ingeniería en Ciencias de la Computación. Se atendió el objetivo mediante tres unidades que abordan conceptos teóricos relacionados con la ingeniería social, la psicología humana y las técnicas de mitigación para responder a las estrategias engañosas que se pueden utilizar.

4. PERFIL DESEABLE DEL PROFESOR (A) PARA IMPARTIR LA ASIGNATURA:

Disciplina profesional:	Ciencias de la Computación o área afín
Nivel académico:	Mínimo Maestría
Experiencia docente:	Mínimo 2 años

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Lilia Mantilla

Daniel M. González Arriaga

Benemérita Universidad Autónoma de Puebla

Vicerrectoría de Docencia

Dirección de Educación Superior

Facultad de Ciencias de la Computación



Experiencia profesional: Mínimo 1 año

5. OBJETIVO:

Aplicar técnicas y conocimientos de ingeniería social con el fin de identificar vulnerabilidades humanas en sistemas de información, para mitigar riesgos y proteger activos digitales contra ataques mediante el empleo de estrategias prácticas, fomentando una actitud ética en el uso de estas técnicas dentro del ámbito de la seguridad cibernética.

6. CONTENIDO

Unidad de Aprendizaje 1: Fundamentos de Ingeniería Social
Contenido Temático
1.1 Definición y Conceptos Básicos
1.1.1 Servicios de Ciberseguridad
1.1.1.1 Autenticación
1.1.1.2 Confidencialidad
1.1.1.3 Disponibilidad
1.1.1.4 Integridad
1.1.1.5 No repudio
1.2 Clasificación de Ataques según el alcance del daño
1.2.1 Ataques Activos
1.2.2 Ataques Pasivos
1.2.3 Ataques de Seguimiento
1.3 Ingeniería social en informática
1.3.1 Origen y evolución del término
1.3.2 El error humano en Ingeniería Social
1.3.3 Principios de la Ingeniería social

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Lilic Mantillo Parvies

Benemérita Universidad Autónoma de Puebla
Vicerrectoría de Docencia
Dirección de Educación Superior
Facultad de Ciencias de la Computación



1.3.3.1 Aspectos legales
1.3.3.2 Aspectos éticos
Referencias: Anderson, R. (2020). Security Engineering: A guide to building dependable distributed systems (3rd ed.). Wiley. Kurose, J., & Ross, K. W. (2010). Redes de computadoras (Vol. 5). Pearson educación. Nota: Este libro se considera un clásico del área de la Ingeniería Social Astudillo Barahona, K. (2017). Hacking Wireless 101: ¡Cómo Hackear Redes Inalámbricas Fácilmente! España: CreateSpace Independent Publishing Platform. Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "{My} data just goes {Everywhere:}" user mental models of the internet and implications for privacy and security. In Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (pp. 39-52). Martin, J. P., Emberley, A. C., Douglas, K., & Soto-Perez, R. (2022). Engineering students' social networks and alters during the COVID-19 pandemic. International Journal of Engineering Education, 38(5), 1643-1659. Mitnick, K. D., Simon, W. L. (2007). El arte de la intrusión: la verdadera historia de las hazañas de hackers, intrusos e impostores. Alfaomega. Nota: El libro se considera adecuado porque incluye historias ficticias acerca de acciones de ataques por ingeniería social, las cuales ejemplifican el concepto de ataques por ingeniería social.
Unidad de Aprendizaje 2: Psicología en la ingeniería social
Contenido Temático: 2.1 Pensamiento adversarial 2.1.1 Definición de pensamiento adversarial 2.1.2 Técnicas de desarrollo de pensamiento adversarial defensivo 2.2 Respuesta emocional en la toma de decisiones 2.2.1 Respuesta emocional 2.2.2 Manipulación de emociones 2.2.3 Estrategias de manejo de respuesta emocional

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Lilia Mantilla Naváez

Daniel M. González Arriaga

Benemérita Universidad Autónoma de Puebla

Vicerrectoría de Docencia

Dirección de Educación Superior

Facultad de Ciencias de la Computación



Lilia Mantillo Nar

2.3 Sesgos cognitivos

2.3.1 Tipos de sesgos cognitivos

2.3.2 Sesgos cognitivos y su impacto en la toma de decisiones

2.3.3 Sesgos cognitivos y su explotación en ataques

2.4 Manipulación y persuasión

2.4.1 Principios de la manipulación y la persuasión

2.4.1.1 Reciprocidad

2.4.1.2 Escasez

2.4.1.3 Autoridad

2.4.1.4 Simpatía

2.4.1.5 Consistencia

2.4.1.6 Consenso

2.4.2 Construcción de confianza

2.4.2.1 Psicología de la confianza

2.4.2.2 Técnicas de construcción de confianza

2.4.2.3 Detección de construcción de confianza malintencionada

2.5 Estrategias de defensa psicológica

2.5.1 Concientización y formación en seguridad

2.5.2 Técnicas para reconocer y resistir la manipulación

2.5.3 Ejemplos de aplicación de estrategias de defensa

Referencias:

Anderson, R. (2020). Security Engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.

Kurose, J., & Ross, K. W. (2010). Redes de computadoras (Vol. 5). Pearson educación.

Nota: Este libro se considera un clásico del área de la Ingeniería Social

Astudillo Barahona, K. (2017). Hacking Wireless 101: ¡Cómo Hackear Redes Inalámbricas Fácilmente! España: CreateSpace Independent Publishing Platform.

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.



Techio, E. M. (2023). Social psychology and different aspects of psychosocial violence in the Brazilian context. PSOCIAL, 9(1), 1-3.

Unidad de Aprendizaje 3: Estrategias engañosas y mitigación

Contenido Temático

- 3.1. Ataques basados en contacto humano
- 3.2. Ataques por computadora
 - 3.2.1 Suplantación
- 3.3. Elementos de verificación
 - 3.3.1 Similitud
 - 3.3.2 Concordancia de circunstancias
- 3.4. Detección y mitigación de ataques de ingeniería social
- 3.5. Controles de seguridad
 - 3.5.1 Preventivo-Detectivo / administrativo
 - 3.5.2. Preventivo-Detectivo / técnico
 - 3.5.3. Preventivo-Detectivo / físico
- 3.6. Aplicación de herramientas
 - 3.6.1. Simulación de entornos de ataques de ingeniería social.
 - 3.6.2 Filtrado de correo electrónico
 - 3.6.3. Listas negras
 - 3.6.4. Herramientas de gestión de eventos e información de seguridad (SIEM) e IDS/IPS.

Referencias:

- Blankenship, R. J. (Ed.). (2021). Deep fakes, fake news, and misinformation in online teaching and learning technologies. IGI Global.
- Kurose, J., & Ross, K. W. (2010). Redes de computadoras (Vol. 5). Pearson educación.
Nota: Este libro se considera un clásico del área de la Ingeniería Social
- Astudillo Barahona, K. (2017). Hacking Wireless 101: ¡Cómo Hackear Redes Inalámbricas Fácilmente! España: CreateSpace Independent Publishing Platform.
- Weidinger, L., Mellor, J., Rauh, M., Griffin, C., Uesato, J., Huang, P. S., & Gabriel, I. (2021). Ethical and social risks of harm from language models. arXiv preprint arXiv:2112.04359.
<https://arxiv.org/abs/2112.04359>.

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Lilia Mantilla Navarrete
Daniel M. González Arriaga

Benemérita Universidad Autónoma de Puebla

Vicerrectoría de Docencia

Dirección de Educación Superior

Facultad de Ciencias de la Computación



Alharbi, S. (2023). Ensemble Defense System: Combining Signature-Based and Behavioral-Based Intrusion Detection Tools. University of Delaware.

Nota: Las referencias deben ser amplias y actuales (no mayor a cinco años)

7. CONTRIBUCIÓN DEL PROGRAMA DE ASIGNATURA AL PERFIL DE EGRESO *(Elegir aquellos que se describen en el perfil de egreso y como se desarrollan en esta asignatura)*

Perfil de egreso			
Conocimientos	Habilidades	Actitudes y valores	Criterios SEAES
Seguridad Informática básica Entenderá cómo funciona la ingeniería social es esencial para diseñar medidas de seguridad efectivas y educar a los usuarios sobre las amenazas potenciales.	Capacidad para resolver problemas basados en sistemas computacionales Identificar y mitigar los riesgos de la ingeniería social requiere habilidades para analizar problemas de seguridad desde la perspectiva humana y tecnológica. Flexibilidad y adaptación Adaptarse a nuevas amenazas y desarrollar estrategias para contrarrestar las tácticas de ingeniería social es crucial en un	Actitudes Compromiso Mostrar compromiso con la seguridad al estar constantemente informado sobre las nuevas técnicas de ingeniería social y proactivamente tomar medidas para prevenirlas. Liderazgo Para dar solución a problemas planteados en simulaciones y escenarios prácticos, liderando su grupo de trabajo al manejar debates y discusiones donde se proporcione retroalimentación	

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Benemérita Universidad Autónoma de Puebla

Vicerrectoría de Docencia

Dirección de Educación Superior

Facultad de Ciencias de la Computación



Perfil de egreso			
Conocimientos	Habilidades	Actitudes y valores	Criterios SEAES
	entorno de seguridad en constante evolución. Pensamiento Creativo La ingeniería social requiere un pensamiento innovador tanto para diseñar ataques como para defenderse de ellos. Desarrollar soluciones creativas para prevenir ataques de ingeniería social es una habilidad valiosa. Razonamiento lógico y crítico Analizar incidentes de ingeniería social y entender los métodos utilizados requiere habilidades de razonamiento lógico y crítico.	constructiva para poder colaborar en proyectos. Valores Honestidad Se enfatizará la seguridad y privacidad de la información, así como la promoción de buenas prácticas, también la promoción de la transparencia y la honestidad, además del respeto a la propiedad intelectual. El desarrollo de tecnologías emergentes en el área de redes, como son la virtualización, la nube, la inteligencia artificial aplicada a la seguridad entre otras, requiere que los estudiantes tengan que mantenerse en formación continua. Responsabilidad	

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Lilia Mant

Daniel M. Gonzalez Arrio

Benemérita Universidad Autónoma de Puebla

Vicerrectoría de Docencia

Dirección de Educación Superior

Facultad de Ciencias de la Computación



Lilia Mantilla Navas

Perfil de egreso			
Conocimientos	Habilidades	Actitudes y valores	Criterios SEAES
		En el desarrollo de proyectos se les promoverá la concientización de minimizar el impacto medioambiental de las TIC (eficiencia energética de la infraestructura, gestión responsable de residuos electrónicos). Así como, el desarrollo de soluciones tecnológicas que contribuyan al bienestar social y ambiental de la comunidad.	

8. Describa cómo el eje o los ejes transversales contribuyen al desarrollo de la asignatura

Describe cómo se fomenta(n) el eje o los ejes transversales en la asignatura

Eje (s) transversales	Contribución con la asignatura
Formación Humana y Social	Las prácticas se elaboran en equipo fomentando la responsabilidad y respeto entre los integrantes.
Desarrollo de Habilidades en el uso de las Tecnologías de la Información y la Comunicación	Las prácticas se basan en el uso de las tecnologías de la información y la comunicación y la vulnerabilidad que presentan ante los ataques de ingeniería social.
Desarrollo de Habilidades del Pensamiento Complejo	Es preciso conocer y comprender los conceptos asociados a la vulnerabilidad, para estar en posibilidad de analizar las distintas amenazas a las que se enfrenta el usuario y desarrollar estrategias que permitan mitigar dichas amenazas.
Lengua Extranjera	Bibliografía en el idioma inglés

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.



Innovación y Talento Universitario	Se requiere el diseño de estrategias que promuevan la concientización sobre temas de ciberseguridad y su prevención.
Educación para la Investigación	En cada momento se fomenta la curiosidad, el pensamiento crítico y la búsqueda de información en biblioteca o en sitios digitales. Docentes incluyen a los estudiantes en sus proyectos de investigación.

9. ESTRATEGIAS, TÉCNICAS Y RECURSOS DIDÁCTICOS *(de las siguientes estrategias, técnicas y recursos didácticos elegir o agregar los que considere pertinentes utilizar para la asignatura y eliminar aquellos que no utilice)*

Estrategias y Técnicas didácticas	Recursos didácticos
● Aprendizaje colaborativo ● Aprendizaje reflexivo ● Ejercicios dentro de clase ● Ejercicios fuera del aula ● E-learning ● Enseñanza en pequeños grupos ● Exposición audiovisual ● Exposición oral ● Portafolios y documentación de avances ● Prácticas de campo ● Prácticas de taller o laboratorio ● Estudio de casos ● Trabajo de investigación ● Trabajo en equipo	● Impresos (textos): libros, documentos... ● Materiales de laboratorio ● Materiales audiovisuales ● Programas informáticos (CD u on-line) educativos: videojuegos, ● Presentaciones multimedia, enciclopedias, animaciones y simulaciones interactivas ● Software especializado ● Plataformas educativas (LMS) ● Páginas Web, Weblog, tours virtuales, webquest, correo electrónico, chats, foros, unidades didácticas y cursos on-line

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Lilia Mantilla Vanier

Daniel M. González Arriaga

Benemérita Universidad Autónoma de Puebla

Vicerrectoría de Docencia

Dirección de Educación Superior

Facultad de Ciencias de la Computación



10. CRITERIOS DE EVALUACIÓN *(de los siguientes criterios propuestos elegir o agregar los que considere pertinentes utilizar para evaluar la asignatura y eliminar aquellos que no utilice, el total será el 100%)*

Criterios	Porcentaje
• <i>Análisis de casos</i>	10%
• <i>Exámenes</i>	30%
• <i>Examen Departamental</i>	10%
• <i>Informe de prácticas</i>	20%
• <i>Presentación en clase</i>	10%
• <i>Proyecto</i>	20%
<i>Total</i>	100%

11. REQUISITOS DE ACREDITACIÓN

Estar inscrito como alumno en la Unidad Académica en la BUAP.
Asistir como mínimo al 80% de las sesiones para tener derecho a exentar por evaluación continua y/o presentar el examen final en ordinario o extraordinario.
Asistir como mínimo al 70% de las sesiones para tener derecho al examen extraordinario.
Cumplir con las actividades académicas y cargas de estudio asignadas que señale el PE.

Notas:

- La entrega del programa de asignatura, con sus respectivas actas de aprobación, deberá realizarse en formato electrónico, vía oficio emitido por la Dirección o Secretaría Académica, a la Dirección de Educación Superior.
- Se anexan manual de Prácticas de Laboratorio, en el formato predefinido por la Unidad Académica, diseñado por los docentes pertenecientes área de conocimiento a cargo de esta asignatura.

Ingeniería Social

El presente documento es Propiedad Intelectual de la Benemérita Universidad Autónoma de Puebla, conforme a lo previsto en el artículo 8 de su Ley y 126 del Estatuto Orgánico Universitario. Su uso es exclusivo de la Benemérita Universidad Autónoma de Puebla y de los integrantes de la comunidad universitaria, en cumplimiento de los fines de docencia, investigación y extensión de la cultura.

Queda estrictamente prohibida la reproducción total o parcial de su contenido o cualquier uso, distintos a los señalados en el párrafo anterior.

Lilia Mantillo Parv