Datos de identificación		
Nombre del EE: CIBERSEGURIDAD INDUSTRIAL	Área Formativa: Vocacional	
Departamento que da el servicio: Ingeniería Industrial		
Clave:	Modalidad: Presencial	Idiomas: Español
Horas totales al semestre: 80	Valor en créditos: 5	Semestre en que se cursa: 9
Carácter: Obligatorio	Antecedente:	EE subsecuente:
Opciones de promoción: Calificación	Mecanismos alternativos de promoción: Equivalencia	

Presentación

Este curso está diseñado para proporcionar a los estudiantes una comprensión profunda de los conceptos clave y las prácticas esenciales para proteger la información y los sistemas en el entorno digital. A través de cinco unidades didácticas, los estudiantes aprenderán sobre los fundamentos de la ciberseguridad, enfocándose en los principios de confidencialidad, integridad y disponibilidad. El curso culmina en un proyecto final donde los estudiantes aplicarán sus conocimientos para diseñar y evaluar soluciones de ciberseguridad, enfrentando escenarios prácticos y desafíos reales.

Desempeños

Competencias genéricas que se ejercitan	*Unidades de competencia profesionales*
1. Utiliza con eficiencia las tecnologías digitales para la comunicación y la gestión de información académica y profesional, en un entorno de trabajo colaborativo. 2. Interpreta de manera integral el mundo natural y social contemporáneo mediante esquemas científicos de generación y aplicación del conocimiento	8.3. Diseñar algoritmos para el control de sistemas complejos integrando teorías matemáticas y computacionales. 8.4. Proponer sistemas de seguridad para dispositivos mediante uso de técnicas de seguridad de la información. 9.1. Operar procesos de manufactura con conocimientos de herramientas, equipos y tecnología inherente 9.3. Formular proyectos de productos y servicios con viabilidad técnica y financiera

Resultados de Aprendizaje

Al finalizar este curso, los estudiantes serán capaces de identificar y analizar amenazas y vulnerabilidades en sistemas de información, aplicar técnicas de cifrado y control de acceso para proteger la confidencialidad, implementar mecanismos para garantizar la integridad de los datos y diseñar estrategias para mantener la disponibilidad de los sistemas. Además, desarrollarán habilidades para evaluar y responder a incidentes de seguridad, preparando soluciones efectivas para proteger entornos digitales complejos.

Orientación didáctica

El curso se impartirá mediante una combinación de conferencias teóricas, ejercicios prácticos, y estudios de caso que permitirán a los estudiantes aplicar los conceptos aprendidos en situaciones reales. Las clases incluirán discusiones sobre temas actuales en ciberseguridad y el uso de herramientas de software específicas para la evaluación y mitigación de riesgos. La evaluación consistirá en pruebas escritas, trabajos prácticos y un proyecto final que requerirá a los estudiantes desarrollar y defender una solución de ciberseguridad completa, integrando los principios de confidencialidad, integridad y disponibilidad.

Actividades del estudiante		*Actividades del profesor*	
Horas/ semestre	*Actividades*	*Horas/ semestre*	*Actividades*
15	Efectuar lecturas especializadas	15	Observa el proceder del estudiante bajo ambientes controlados
15	Realizar ejercicios	50	Expone la intencionalidad del curso, brindando la información pertinente para el abordaje del curso.
50	Asistencia a clase	15	Revisa ejercicios

Evaluación del aprendizaje

Criterios de cumplimiento	*Evidencias de desempeño*	*Evidencias de conocimiento*
Entrega de prácticas en tiempo y forma. Entrega del proyecto en tiempo y forma. Entrega de tareas en tiempo y forma.	Reporte de proyecto. Reporte de prácticas. Reporte de tareas. Examen. Portafolio de evidencias.	El estudiante es capaz de argumentar sus opiniones de manera lógica y precisa
Técnicas e instrumentos de evaluación	Rúbrica. Formulario de examen.	

Recursos para la formación

Contenidos básicos	*Materiales*
Unidad Didáctica 1: Introducción a la Ciberseguridad 1.1 Conceptos básicos de ciberseguridad 1.2 Historia y evolución de la ciberseguridad 1.3 Tipos de amenazas y ataques cibernéticos	• Pintarrón • Equipo audiovisual • Centro de cómputo • Software Anaconda

1.4 Marcos y estándares de ciberseguridad Unidad Didáctica 2: Confidencialidad 2.1 Cifrado de datos y criptografía 2.2 Control de acceso y autenticación 2.3 Protocolos de seguridad para la protección de la confidencialidad 2.4 Gestión de identidades y políticas de privacidad Unidad Didáctica 3: Integridad 3.1 Conceptos de integridad de datos 3.2 Técnicas de verificación y validación de datos 3.3 Algoritmos de hash y firma digital 3.4 Protección contra alteración y manipulación de información Unidad Didáctica 4: Disponibilidad 4.1 Principios de disponibilidad en sistemas de información 4.2 Estrategias de redundancia y recuperación ante desastres 4.3 Protección contra ataques de denegación de servicio (DoS) 4.4 Monitoreo y gestión de la continuidad del servicio Unidad Didáctica 5: Proyecto Final 5.1 Planificación y definición del proyecto 5.2 Desarrollo de soluciones de ciberseguridad 5.3 Pruebas de seguridad y evaluación de vulnerabilidades 5.4 Presentación y defensa del proyecto	

Bibliografía

1. Stallings, W., & Brown, L. (2020). Computer Security: Principles and Practice (5th ed.). Pearson. ISBN: 978-0134444284
2. Pfleeger, C. P., & Pfleeger, S. L. (2022). Security in Computing (6th ed.). Pearson.ISBN: 978-0134085043
3. Anderson, R. (2021). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley. ISBN: 978-1119642782
4. Schneier, B. (2023). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley. ISBN: 978-1119096722
5. Bishop, M. (2022). Introduction to Computer Security (2nd ed.). Addison-Wesley. ISBN: 978-0134085043

Perfil deseable del profesor que lo conduce o lo coordina

Grado académico: Maestría	Área de formación: Ingeniería en cómputo o afín
Experiencia docente: 1 año	Experiencia profesional en el campo: 1 años
Elaboró: Jesús Horacio Pacheco Ramirez	Fecha: 27 de agosto de 2024