CIENCIA DE LA COMPUTACIÓN

SEGURIDAD EN COMPUTACIÓN

3 CRÉDITOS

UTEC
UNIVERSIDAD DE INGENIERÍA Y TECNOLOGÍA

CE2A

ÍNDICE

UNIVERSIDAD DE INGENIERÍA Y TECNOLOGÍA
SILABO 2021-1

1. ASIGNATURA

CS3I01 - Seguridad en Computación

2. DATOS GENERALES

2.1 Ciclo: 9º
2.2 Créditos: Tres (3) créditos
2.3 Horas de teoría: Una (1) semanales
2.4 Horas de práctica: Cuatro (4) semanales
2.5 Duración del período: Dieciséis (16) semanas
2.6 Condición: Obligatorio
2.7 Modalidad: Virtual
2.8 Requisitos:
- CS2301 Redes y Comunicaciones

3. PROFESORES

3.1 Profesor coordinador del curso

Jose Pazos (jpazos@utec.edu.pe)
Horario de atención: Previa coordinación con el profesor

3.2 Profesor(es) instructor(es) del curso

Jose Pazos (jpazos@utec.edu.pe)
Horario de atención: Previa coordinación con el profesor

4. INTRODUCCIÓN AL CURSO

Los sistemas computacionales guardan mucha información sobre sus usuarios y existen terceros dispuestos a vulnerar estos si no se desarrollan con la ciberseguridad en mente. Ya sea una aplicación Web, un sistema operativo, un compilador, etc., los diseñadores e implementadores tienen que tener un amplio conocimiento de los principios y la práctica de la ciberseguridad para cumplir las expectativas del sistema y de sus usuarios.

5. OBJETIVOS

Sesión 1: Describir el impacto de la ciberseguridad en usuarios y desarrolladores, definir conceptos base de seguridad. Crear algoritmos de cifrado y su realizar su criptoanálisis.

Sesión 2: Definir la seguridad en términos precisos. Describir cifrados de criptografía simétrica modernos: redes-SP, redes de Feistel y modos de operación de bloques.

Sesión 3: Describir el sistema de encriptación AES y códigos de autenticación de mensajes.

Sesión 4: Definir el concepto de función unidireccional. Crear funciones de Hashing y analizar su seguridad.

Sesión 5: Definir el concepto de seguridad asimétrica. Describir procesos de encriptación asimétricos e intercambios de llaves públicas.

Sesión 6: Aplicar la encriptación asimétrica a casos de la vida real. Describir la autenticación de mensajes encriptados asimétricamente.

Sesión 7: Formular principio de diseños de sistemas seguros. Analizar sistemas usando modelamiento de amenazas. Describir modelos comunes de redes y aplicaciones Web.

Sesión 8: Aplicar conceptos de seguridad al control de acceso. Describir diversos métodos de autenticación y sus implementaciones. Analizar los beneficios y fallas de éstos.

Sesión 9: Describir métodos de autorización modernos. Analizar los beneficios y fallas de cada uno. Crear métodos de detección de intrusos.

Sesión 10: Construir modelos del diseño de un sistema de software simple los cuales son apropiado para el paradigma utilizado para diseñarlo.

Sesión 11: Desarrollar protocolos criptográficos para uso en aplicaciones Web.

Sesión 12: Continuación de la sesión 11.

Sesión 13: Definir tipos de ataques comunes en aplicaciones Web. Identificar implementaciones vulnerables y describir pautas para prevenir éstas.

Sesión 14: Implementar soluciones para aplicaciones vulnerables.
Sesión 15: Definir el concepto de seguridad usable. Describir casos en los que los humanos hayan causado vulnerabilidades en software y formas de prevenirlos.

6. COMPETENCIAS Y CRITERIOS DE DESEMPEÑO

Los criterios de desempeño que se van a trabajar en este curso son:

1.1. Aplica conocimientos de matemáticas apropiados para la solución de problemas definidos y sus requerimientos en la disciplina del programa. (*nivel 3*)

4.1. Crea, selecciona, adapta y aplica técnicas, recursos y herramientas modernas para la práctica de la computación y comprende sus limitaciones. (*nivel 3*)

7.2. Analiza y valora el impacto local y global de la computación sobre las personas, las organizaciones y la sociedad. (*nivel 3*)

8.1. Entiende la ética y las responsabilidades profesionales. (*nivel 2*)

7. RESULTADOS DE APRENDIZAJE

Al finalizar el curso de Ingeniería de software se espera que el estudiante sea capaz de:

RA1. Construir algoritmos de cifrado y determinar las propiedades matemáticas que garanticen su seguridad y la probabilidad de vulneración.

RA2. Identificar las propiedades de una solución computacional segura y no segura.

RA3. Construir soluciones computacionales seguras con altos estándares de calidad.

RA4 .Aplicar técnicas de Ethical Hacking para garantizar la seguridad de una solución computacional.

8. TEMAS

1. **Introducción**
    1. ¿Por qué la ciberseguridad?
    2. Impacto de seguridad en usuarios y desarrolladores
    3. Conceptos de seguridad
    4. Autenticación
    5. El rol de los humanos en los sistemas seguros
2. **Criptografía**
    1. Cifrados históricos
    2. Criptografía simétrica
        1. Cifrados de bloque, de flujo, redes SP
        2. Redes de Feistel
        3. Códigos de autenticación de mensaje
        4. AES (Advanced Encryption Standard)
    3. Hashing
    4. Criptografía asimétrica
        1. Motivación y funcionamiento
        2. Protocolos de intercambio de llaves
        3. Encriptación asimétrica
        4. Firmas criptográficas

3. **Diseño de sistemas seguros**
    1. Introducción
        1. Principios de diseño de ciberseguridad
        2. Modelado de amenazas
        3. Modelos de aplicaciones Web
    2. Control de acceso
        1. Motivación
        2. Autenticación
        3. Protocolos de autenticación
    3. Autorización
        1. Listas de control de acceso
        2. Capabilities
        3. Detección de intrusos
    4. Criptografía aplicada
        1. Protocolos criptográficos
        2. TLS
        3. OAuth
        4. Cifrado de extremo a extremo

4. **Vulnerabilidades, exploits y humanos**
    1. Exploits del mundo real
        1. Buffer overflow
        2. XSS
        3. DoS
        4. Ataques de inyección
    2. Seguridad usable (Si el tiempo lo permite)
        1. El factor humano en la seguridad
        2. Reuso de contraseñas
        3. CSRF
        4. Verificación de certificados
        5. El factor económico

9. PLAN DE TRABAJO

9.1 Metodología

Este curso presenta por metodología activa el aprendizaje clásico y el aprendizaje basado en problemas; ambos son fundamentales para introducir al estudiante a los conceptos básicos y afianzar la base necesaria para los siguientes cursos de carrera. Ambos aumentan el interés del estudiante y promueven su compromiso en el aprendizaje.

9.2 Sesiones de teoría

Las sesiones de teoría se llevan a cabo en clases magistrales donde se realizarán actividades que propicien un aprendizaje activo, con dinámicas que permitan a los estudiantes interiorizar los conceptos. Se fomenta la participación individual y en equipo para exponer sus ideas, motivándolos con puntos adicionales en las diferentes etapas de la evaluación del curso.

9.3 Sesiones de práctica (laboratorio o taller)

En las sesiones de laboratorio se propondrán problemas para verificar que los alumnos hayan alcanzado el logro planteado para cada una de las unidades de aprendizaje, estas actividades les permitirá aplicar los conocimientos adquiridos durante las sesiones de teoría y además estos retos permitirá la evaluación del desempeño de los alumnos.

10. SISTEMA DE EVALUACIÓN

Parte de la evaluación continua serán presentaciones grupales, y prácticas individuales en clase y laboratorio. Las prácticas en clase serán presentadas el mismo día salvo algunas excepciones. Mientras que las prácticas de laboratorio tendrán una fecha de entrega.

EVALUACIÓN *La ponderación de la evaluación se hará si ambas partes están aprobadas	**TEORÍA (T)**	**LABORATORIO (L)**
	Evaluación Continua (**C1**) (10%) Evaluación Continua (**C2**) (10%) Examen Final (**E1**) (20%)	Proyecto Parcial (**P1**) (20%) Proyecto Parcial (**P2**) (20%) Proyecto Final (**P3**) (20%)
	40%	60%
	100%	

Las rúbricas que permitirán medir las actividades más significativas del curso y que, además se relacionan con la evaluación de las competencias del estudiante son: enlace

11. SESIONES DE APOYO O TUTORÍAS

Este apartado permite formalizar los espacios de apoyo a los estudiantes y que éstos tengan la atención NECESARIA y el tiempo disponible para presentar sus dudas y consultas acerca del curso:

12. REFERENCIAS BIBLIOGRÁFICAS

- Stamp, M. (2011). Information Security: Principles and practice. 2nd Edition. Wiley.
- van Oorschot, P. (2020). Computer Security and the Internet. Tools and Jewels. 1st edition. Springer.
- Katz, J., Lindell, Y. (2014). Introduction to modern cryptography. 2nd edition. CRC Press.

- Eriksson, H. E., Penker, M., Lyons, B., & Fado, D. (2003). UML 2 Toolkit, CafeScribe (Vol. 26). John Wiley & Sons.