



UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE: INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE: Software

MODALIDAD PRESENCIAL

SÍLABO

SEGURIDAD EN EL DESARROLLO DEL SOFTWARE

NIVEL

OCTAVO

AMBATO - ECUADOR
2026

I. INFORMACIÓN GENERAL

Nombre de la asignatura SEGURIDAD EN EL DESARROLLO DEL SOFTWARE Carrera Software		
Código UTA-FISEI-SF-MP-UP-08-03	PRERREQUISITOS	
Modalidad PRESENCIAL	Asignatura	Código
	GESTION DE CALIDAD DEL SOFTWARE	UTA-FISEI-SF-MP-UP-07-05
Unidad organizacional curricular PROFESIONAL		
Créditos/Horas 3 Nivel OCTAVO	CORREQUISITOS	
	Asignatura	Código
CARGA HORARIA		
Componente de aprendizaje en contacto con el docente por semana 3	Componente de aprendizaje en contacto con el docente por ciclo académico 48	Componente de aprendizaje práctico experimental, componente de aprendizaje autónomo 96
Horas de tutoría académica semanales 1	Horas de tutoría presenciales por ciclo académico 16	Horas de tutorías virtuales por ciclo académico 0

TOTAL DE HORAS DE APRENDIZAJE EN EL CICLO DE ESTUDIOS

Número de horas del componente de aprendizaje en contacto con el docente semanal	3
Número de horas del componente de aprendizaje en contacto con el docente semestral	48
Número de horas del componente de aprendizaje práctico experimental y componente de aprendizaje autónomo	96
TOTAL DE HORAS AL SEMESTRE (Número de horas del componente de aprendizaje en contacto con el docente semestral + Número de horas del componente de aprendizaje práctico experimental y componente de aprendizaje autónomo.)	144

III DESCRIPCIÓN Y OBJETIVOS DE LA ASIGNATURA

Propósito La seguridad es un aspecto fundamental para el funcionamiento del software. Esta debe tenerse en cuenta durante todo el ciclo de vida del desarrollo del software, desde las etapas tempranas hasta la puesta a punto y su mantenimiento. Con este módulo se pretende desarrollar habilidades en el desarrollo seguro del software, identificar problemas de la seguridad informática que se enfrentan e implementar posibles soluciones a estos.

Descripción de la asignatura La asignatura Seguridad en el Desarrollo del Software integra fundamentos teóricos y prácticos para la construcción de aplicaciones seguras a lo largo del ciclo de vida del desarrollo del software, abordando principios de seguridad informática, protección de bases de datos, autenticación y control de acceso, identificación y mitigación de vulnerabilidades en aplicaciones web, y el uso de herramientas y buenas prácticas para el desarrollo seguro. El proceso de enseñanza aprendizaje se desarrolla mediante metodologías activas como el aprendizaje basado en proyectos, resolución de problemas y actividades prácticas de laboratorio, promoviendo el análisis, la aplicación de estándares de seguridad y la implementación de soluciones en escenarios reales. Al finalizar la asignatura, el estudiante será capaz de identificar riesgos y vulnerabilidades, aplicar controles de seguridad en aplicaciones y emplear herramientas y prácticas de programación segura para mitigar amenazas en entornos de desarrollo de software.

Objetivo general de la asignatura Aplicar fundamentos y estándares de seguridad en el proceso de desarrollo de software para mitigar el riesgo de la ocurrencia de fallos

Objetivos específicos de la asignatura

- 1.-Conocer las bases teóricas de la seguridad informática
- 2.-Desarrollar habilidades en el desarrollo seguro del software
- 3.-Identificar y solucionar las principales vulnerabilidades y tipos de ataque en entorno web
- 4.-Conocer herramientas de apoyo al desarrollo seguro del software.

NOTA: Las horas de tutoría académica no se suman, por lo tanto no se incluyen dentro de las horas totales del semestre

IV PROGRAMA DE ESTUDIOS DE LA ASIGNATURA

U.1	Conocer las bases teóricas de la seguridad informática			
Unidades temáticas	Horas Clase / Componente de aprendizaje en contacto con el docente	Componente de aprendizaje práctico experimental.	Componente de aprendizaje autónomo incluidas las actividades de investigación y vinculación con la sociedad	Instrumentos de evaluación
1.1.- Principios de la seguridad informática. Panorama nacional e internacional de la seguridad informática.	3	3	3	Evaluaciones escritas u orales en actividades practicas
1.2.- Teoría de la información	3	3	3	Evaluaciones Parciales Pruebas escritas de la unidad
SUBTOTAL HORAS	6	6	6	TOTAL HORAS: 18

Resultados de aprendizaje: Conoce las bases teóricas de la seguridad informática
Metodología de enseñanza : Aprendizaje Basado en Proyectos, Método expositivo
Estrategias educativas : Lectura, análisis y comprensión de materiales bibliográficos y documentales, Trabajos y exposiciones
Recursos didácticos : Marcadores, Proyector, Audiovisuales, Internet, Inteligencia Artificial, Tecnología del Aprendizaje y el Conocimiento
Habilidades Blandas : Trabajo en equipo, Responsabilidad

IV PROGRAMA DE ESTUDIOS DE LA ASIGNATURA

U.2	Desarrollar habilidades en el desarrollo seguro del software			
Unidades temáticas	Horas Clase / Componente de aprendizaje en contacto con el docente	Componente de aprendizaje práctico experimental.	Componente de aprendizaje autónomo incluidas las actividades de investigación y vinculación con la sociedad	Instrumentos de evaluación
2.1.- La seguridad en las bases de datos	9	9	9	Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
2.2.- La seguridad en el levantamiento de requisitos.	3	3	3	Trabajos y ejercicios en clases Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
2.3.- Autenticación del usuario.	3	3	3	Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
2.4.- Control de acceso	3	3	3	Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
SUBTOTAL HORAS	18	18	18	TOTAL HORAS: 54

Resultados de aprendizaje: Desarrolla habilidades en el desarrollo seguro del software

Metodología de enseñanza : Aprendizaje Basado en Proyectos, Método expositivo

Estrategias educativas : Conferencias , Actividades académicas desarrolladas en escenarios experimentales o en laboratorios, Trabajos y exposiciones

Recursos didácticos : Marcadores, Proyector, Audiovisuales, Internet, Inteligencia Artificial, Tecnología del Aprendizaje y el Conocimiento

Habilidades Blandas : Trabajo en equipo, Responsabilidad

IV PROGRAMA DE ESTUDIOS DE LA ASIGNATURA

U.3	Identificar y solucionar las principales vulnerabilidades y tipos de ataque en entorno web			
Unidades temáticas	Horas Clase / Componente de aprendizaje en contacto con el docente	Componente de aprendizaje práctico experimental.	Componente de aprendizaje autónomo incluidas las actividades de investigación y vinculación con la sociedad	Instrumentos de evaluación
3.1.- Ataques a aplicaciones web	6	6	6	Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
3.2.- Detección de vulnerabilidades web	6	6	6	Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
3.3.- Solución a vulnerabilidades web	3	3	3	Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
SUBTOTAL HORAS	15	15	15	TOTAL HORAS: 45

Resultados de aprendizaje: Identifica y soluciona las principales vulnerabilidades y tipos de ataque en entorno web

Metodología de enseñanza : Aprendizaje Basado en Proyectos, Método expositivo

Estrategias educativas : Actividades académicas desarrolladas en escenarios experimentales o en laboratorios, Resolución de problemas, Trabajos y exposiciones

Recursos didácticos : Marcadores, Proyector, Audiovisuales, Internet, Inteligencia Artificial, Tecnología del Aprendizaje y el Conocimiento

Habilidades Blandas : Trabajo en equipo, Responsabilidad

IV PROGRAMA DE ESTUDIOS DE LA ASIGNATURA

U.4	Conocer herramientas de apoyo al desarrollo seguro del software.			
Unidades temáticas	Horas Clase / Componente de aprendizaje en contacto con el docente	Componente de aprendizaje práctico experimental.	Componente de aprendizaje autónomo incluidas las actividades de investigación y vinculación con la sociedad	Instrumentos de evaluación
4.1.- Control de versiones	3	3	3	Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
4.2.- Patrones de diseño.	3	3	3	Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
4.3.- Programación limpia.	3	3	3	Evaluaciones escritas u orales en actividades practicas Pruebas escritas de la unidad
SUBTOTAL HORAS	9	9	9	TOTAL HORAS: 27

Resultados de aprendizaje: Conoce herramientas de apoyo al desarrollo seguro del software

Metodología de enseñanza : Aprendizaje Basado en Proyectos, Método expositivo

Estrategias educativas : Actividades académicas desarrolladas en escenarios experimentales o en laboratorios, Resolución de problemas, Trabajos y exposiciones

Recursos didácticos : Marcadores, Proyector, Audiovisuales, Internet, Inteligencia Artificial, Tecnología del Aprendizaje y el Conocimiento

Habilidades Blandas : Trabajo en equipo, Responsabilidad

V ESCENARIOS DE APRENDIZAJE (REAL, VIRTUAL, ÁULICO)

Escenario Real: Comprende actividades de aprendizaje en laboratorio Escenario Aulico: Actividades de enseñanza aprendizaje, desarrolladas en el aula Escenario Virtual: Uso de la computadora, aula virtual, simuladores

VI CRITERIOS NORMATIVOS PARA LA EVALUACIÓN

Objetivos específicos	Evaluación diagnóstica (Conocimientos previos)	Evaluación formativa (Grado de logro de destrezas)	Evaluación sumativa (valorar los objetivos generales alcanzados y el logro de destrezas)
1.- Conocer las bases teóricas de la seguridad informática	Preguntas de sondeo sobre la Unidad	RÚBRICA	Examen del parcial.
2.- Desarrollar habilidades en el desarrollo seguro del software	Preguntas de sondeo sobre la Unidad	RÚBRICA	Examen del parcial.
3.- Identificar y solucionar las principales vulnerabilidades y tipos de ataque en entorno web	Preguntas de sondeo sobre la Unidad	RÚBRICA	Examen de fin de parcial.
4.- Conocer herramientas de apoyo al desarrollo seguro del software.	Preguntas de sondeo sobre la Unidad	RÚBRICA	Examen de fin de parcial.

VII BIBLIOGRAFÍA

BIBLIOGRAFÍA BÁSICA

Autores	Año	Título	Nro Edición	Editorial	Pais o Ciudad	Nro Ejemplares	Nro Páginas	Tipo
Ortega Candel; José Manuel		Desarrollo seguro en ingeniería del software:	1a edición			6	386 páginas	Físico
Código/Ubicación base de datos:	BFISEI3039a							
Comentario:	Aplicaciones seguras con android, NodeJS, Python y C++							
URL:								

Autores	Año	Título	Nro Edición	Editorial	Pais o Ciudad	Nro Ejemplares	Nro Páginas	Tipo
Hernández Bejarno, Miguel	2020	Ciclo de vida de desarrollo ágil de software seguro	1	Fundacion Universitaria Los Libertadores	Colombia Bogota	1	121	Virtual
Código/Ubicación base de datos:								
Comentario:	Aborda ciclo de vida de desarrollo ágil de software seguro es un libro resultado de un proyecto de investigación donde confluyen e integran tres grandes temáticas relacionadas con la construcción de software seguro: desarrollo ágil, buenas prácticas y seg							
URL:	https://0x102pmad-y-https-elibro-net.itmsp.museknowledge.com/es/ereader/uta/197008							

BIBLIOGRAFÍA COMPLEMENTARIA

Autores	Año	Título	Nro Edición	Editorial	País/Ciudad	Nro Ejemplares	Nro Páginas	Tipo
Pantaleo ;Guillermo	2016	Calidad en el desarrollo de software	2a edición	Alfaomega	Buenos Aires	3	247 páginas	Físico
Código/Ubicación base de datos:	BFISEI1686a							
Comentario:	Este libro es una guía completa y practica para la creación de consultas, formularios o informes complejos, pasando por apartados importantes como la integridad referencial, las consultas SQL, la seguridad o la importación y exportación de archivos.							
URL:								

