PROGRAMA DE ASIGNATURA - SÍLABO

1. DATOS GENERALES

Modalidad: PRESENCIAL ESPE LTGA-G RODRIGUEZ LARA	**Departamento:** CIENCIAS DE LA COMPUTACION		**Área de Conocimiento:** SISTEMAS DE INFORMACION	
Nombre Asignatura: DESARROLLO DE SOFTWARE SEGURO	**Período Académico:** PREGRADO S-II OCT21-MAR22			
Fecha Elaboración: 20/05/21 03:56 PM	**Código:** A0G19	**NRC:** 8935		**Nivel:** PREGRADO
Docente: LOPEZ OTAÑEZ EDGAR RUBEN erlopez5@espe.edu.ec				

Unidad de Organización	PROFESIONAL
Campo de Formación:	PRAXIS PROFESIONAL
Núcleos Básicos de	Fundamentos de seguridad informática Mecanismos de seguridad Aplicaciones de la seguridad de la información

CARGA HORARIA POR COMPONENTES DE APRENDIZAJE			SESIONES SEMANALES
DOCENCIA	**PRACTICAS DE APLICACIÓN Y EXPERIMENTACIÓN**	**APRENDIZAJE AUTÓNOMO**	2
32	32	32	

Fecha Elaboración	Fecha de Actualización	Fecha de Ejecución
20/05/2021	20/05/2021	17/05/2021

Descripción de la Asignatura:

Esta asignatura analiza los aspectos de desarrollo de software cuando se trata de desarrollar un sistema software que debe tener la propiedad de ser seguro.

Contribución de la Asignatura:

Esta asignatura permitirá conocer y aplicar los procesos, modelos, normas y estándares de seguridad para garantizar la integridad, seguridad y fiabilidad de los datos en un sistema software.

Resultado de Aprendizaje de la Carrera: (Unidad de Competencia)

Reconoce los principios fundamentales de la Ingeniería de Software a través de la elaboración de algoritmos, pseudocódigo, pruebas de escritorio y codificación de programas básicos de computadores con pensamiento lógico y creativo a fin de solucionar problemas en diferentes dominios.
Desarrollar sistemas software seguros aplicando en el proceso de desarrollo de software para garantizar la integridad, seguridad y fiabilidad de los datos al usuario final de la aplicación software

Objetivo de la Asignatura: (Unidad de Competencia)

Formar profesionales en Ingeniería de Software capaces de aplicar modelos, normas y estándares necesarios para obtener productos y procesos software de alta calidad que garanticen el cumplimiento de requerimientos, demostrando creatividad, eficiencia, eficacia y responsabilidad profesional; con el propósito de contribuir a la innovación tecnológica en las organizaciones y a la mejora de los sectores productivos del País.
Esta asignatura corresponde a la primera etapa del eje de formación profesional, proporciona al futuro profesional las bases conceptuales para garantizar la calidad del proceso y producto del desarrollo del software

Resultado de Aprendizaje de la Asignatura: (Elemento de Competencia)

Comprender la ciencia detrás de los sistemas de información basados en la Web y los principios de ingeniería de los sistemas de Información Web.
Efectúa análisis sobre los componentes software necesarios en proyectos de desarrollo de sistemas Web para con ello lograr la implementación recuperación de la información web y extracción de la información aplicado en la web para análisis de información.
Conoce los componentes, arquitectura, tecnología y la seguridad que se puede dar en las aplicaciones Web, para tomar medidas respectivas de los posibles ataques que se pueden producirse en las mismas.
Aplica, discute y reconoce de forma efectiva las diferentes medidas para evitar los posibles ataques en las aplicaciones web.

Participa pro-activamente en un equipo de trabajo, resolviendo problemas que empleen conceptos de seguridad en las aplicaciones web. Integrar los conceptos utilizados en el diseño, desarrollo y el despliegue de aplicaciones basadas en la Web mostrando participación activa como parte de trabajo colaborativo en diferentes casos de estudios.

Proyecto Integrador

PERFIL SUGERIDO DEL DOCENTE

TÍTULO Y DENOMINACIÓN

GRADO: Ingeniero en Sistemas y/o Software y/o Informática

POSGRADO: Doctor en Ingeniería de Software y/o Sistemas y/o Informática

2. SISTEMA DE CONTENIDOS Y RESULTADOS DEL APRENDIZAJE

CONTENIDOS		
Unidad 1 **Horas/Min:** 22:00	**HORAS DE TRABAJO AUTÓNOMO**	
Introducción y Estudio de Vulnerabilidades	Prácticas de Aplicación y Experimentación	
Introducción		
Qué es la seguridad del Software		
La importancia de la seguridad en el Software		
Las vulnerabilidades y sus costes	**Tarea 1**	Consulta tipos de vulerabilidades del Software
Gestión de riesgos de seguridad del software	**Tarea 2**	Consulta Riesgos de Seguridad del software
Propiedades del software seguro y resiliente		
Conceptos de seguridad	**Tarea 3**	Consulta Terminología en la Seguridad del Software
Amenazas a la seguridad del software		
Amenazas a nivel de Hardware		
Amenazas a nivel de Código	**Laboratorio 1**	Identificar vulnerabilidades en un fragmento de código
	Tarea 4	Ejemplificar una amenaza a nivel de código
Amenazas a nivel de Diseño		
Amenazas a nivel de Arquitectura		
Plan estratégico		
Seguridad y resiliencia a lo largo del ciclo de vida de desarrollo de Software(SDLC)	**Laboratorio 2**	Identificar las vulnerabilidades dentro de un proyecto de software
Directrices de seguridad adicionales		
Soluciones/Frameworks de seguridad de software existentes	**Laboratorio 3**	Taller uso de Frameworks
Puntos de ataque y seguridad perimetral		

ACTIVIDADES DE APRENDIZAJE / HORAS CLASE	
COMPONENTES DE DOCENCIA	16
PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	8
HORAS DE TRABAJO AUTONOMO	8
TOTAL HORAS POR UNIDAD	**32**

CONTENIDOS		
Unidad 2 **Horas/Min:** 21:00	**HORAS DE TRABAJO AUTÓNOMO**	
Diseño de aplicaciones seguras y resilientes	Prácticas de Aplicación y Experimentación	
Diseño de Software Seguro		

2. SISTEMA DE CONTENIDOS Y RESULTADOS DEL APRENDIZAJE

Casos de abuso		
Modelado de amenazas y riesgos	**Tarea 1**	Modelar amenazas de seguridad
Defensa en profundidad		
Codificación Segura y Programación Defensiva		
Evolución de los ataques		
Taxonomías de amenazas y vulnerabilidades		
Validación y manejo de entradas	**Laboratorio 1**	Taller validación de entradas
Mejores prácticas en la validación de los datos de entrada	**Laboratorio 2**	Taller de implementación de mejores prácticas para la validación de entradas
Buenas prácticas según OWASP (Open Web Application Security Project)	**Tarea 2**	Consulta de recomendaciones de la OWASP

ACTIVIDADES DE APRENDIZAJE / HORAS CLASE	
COMPONENTES DE DOCENCIA	16
PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	8
HORAS DE TRABAJO AUTONOMO	8
TOTAL HORAS POR UNIDAD	**32**

CONTENIDOS		
Unidad 3 **Horas/Min:** 21:00	**HORAS DE TRABAJO AUTÓNOMO**	
Pruebas de seguridad	Prácticas de Aplicación y Experimentación	
Pruebas y seguridad		
Tipos de análisis estático		
Herramientas de análisis	**Laboratorio 1**	Taller de análisis estático de código
Tipos de análisis dinámico		
Herramientas de análisis dinámico	**Laboratorio 2**	Taller de análisis dinámico de código
Pruebas		
Buenas prácticas de pruebas de unidades	**Laboratorio 3**	Taller de implementación de pruebas unitarias
Pruebas de penetración	**Laboratorio 4**	Taller de pruebas de penetración
Fuzzing	**Laboratorio 5**	Taller de Fuzzing
Avances recientes y perspectivas de futuro		
AVANCES RECIENTES Y PERSPECTIVAS DE FUTURO		

ACTIVIDADES DE APRENDIZAJE / HORAS CLASE	
COMPONENTES DE DOCENCIA	16
PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	8
HORAS DE TRABAJO AUTONOMO	8
TOTAL HORAS POR UNIDAD	**32**

3. PROYECCIÓN METODOLÓGICA Y ORGANIZATIVA PARA EL DESARROLLO DE LA

Metodos de Enseñanza - Aprendizaje

1. Talleres
2. Clase Magistral
3. Resolución de Problemas
4. Prácticas de Laboratorío

Empleo de Tics en los Procesos de Aprendizaje	
1	Herramientas Colaborativas (Google, drive, onedrives, otros)
2	Material Multimedia
3	Software de Simulación
4	Aula Virtual

4. RESULTADOS DEL APRENDIZAJE, CONTRIBUCIÓN AL PERFIL DEL EGRESO Y TÉCNICA DE

PROYECTO INTEGRADOR DEL NIVEL RESULTADO DE APRENDIZAJE POR UNIDAD CURRICULAR	Niveles de logro: Alta(A), Media (B), C(Baja).	ACTIVIDADES INTEGRADORAS
1. Conocer qué es la seguridad del software y su importancia, saber identificar los diferentes tipos de vulnerabilidades y amenazas a las que están expuestas las aplicaciones y como prevenirlas y gestionarlas	Alta A	Analizar casos de ataques a la seguridad del software y sus consecuencias, Talleres de discución para identificar las vulnerabilidades y amenazas a las aplicaciones.
2. Identificar y conocer las principales causas de vulnerabilidad conocidas. Integrar la seguridad en el ciclo de vida de desarrollo de software seguro	Alta A	Modelamiento de las amenazas a la seguridad. Taller de codificación segura, taller de validación de entradas
3. Conocer las pruebas que se pueden aplicar para obtener un producto software resiliente y seguro.	Alta A	Implementar y aplicar pruebas de seguridad usando frameworks y herramientas

6. TÉCNICAS Y PONDERACION DE LA EVALUACIÓN

Técnica de evaluación	1er Parcial	2do Parcial	3er Parcial
Pruebas oral/escrita	6	6	6
Talleres	4	4	4
Examen Parcial	6	6	6
Tareas o guías	4	4	4
TOTAL:	**20**	**20**	**20**

7. BIBLIOGRAFÍA BÁSICA/ TEXTO GUÍA DE LA ASIGNATURA

Titulo	Autor	Edición	Año	Idioma	Editorial
INFORMATION TECHNOLOGY CONVERGENCE, SECURE AND TRUST COMPUTING, AND DATA MANAGEMENT	-	-	-	-	-
Information technology convergence, secure and trust computing, and data management ITCS 2012 & STA 2012	[sin autor]	-	2012	eng	Springer Netherlands
ENGINEERING SECURE SOFTWARE AND SYSTEMS	-	-	-	-	-

8. BIBLIOGRAFÍA COMPLEMENTARIA

Titulo	Autor	Edición	Año	Idioma	Editorial
SECURE, RESILIENT, AND AGILE SOFTWARE DEVELOPMENT	Mark S. Merkow	1	2020	Ingles	CRC Press
SOFTWARESECURITY:BUILDING SECURESOFTWAREAPPLICATIONS	Neha Kaul	Neha Kaul	2020	Ingles	Arcler Press

9. LECTURAS PRINCIPALES

Tema	Texto	Página	URL
Desarrollo de software Seguro	Artículo	Todo	http://polux.unipiloto.edu.co:8080/00001900.pdf
Desarrollo de Software seguro	Web	todo	https://owasp.org/www-pdf-archive/Desarrollo_Seguro_Principios_y_Buenas_Pr%C3%A1cticas..pdf

10. ACUERDOS

Del Docente:

1. Esforzarme en conocer con amplitud al campo académico y práctico
2. Asistir a clases siempre y puntualmente dando ejemplo al estudiante para exigirle igual comportamiento
3. Motivar, estimular y mostrar interés por el aprendizaje significativo de los estudiantes y evaluar a conciencia y con justicia
4. Mantener en todo momento un clima de empatía y consideración entre estudiantes, profesores, administrativos, trabajadores, etc.
5. Cumplir con las leyes y reglamentos institucionales y orientar todos los esfuerzos en la dirección de los grandes propósitos de la Universidad (Misión, Visión)
6. Cumplir con las obligaciones de estudiantes y docentes para devengar la inversión que hace el estado Ecuatoriano en favor de los mismos.

De los Estudiantes:

1. Ser honesto, no copiar, no mentir
2. Colaborar con los eventos programados por la institución e identificarme con la carrera
3. Mantener en todo momento un clima de empatía y consideración entre estudiantes, profesores, administrativos, trabajadores, etc.
4. Cumplir con las leyes y reglamentos institucionales y orientar todos los esfuerzos en la dirección de los grandes propósitos de la Universidad (Misión, Visión)
5. Cumplir con las obligaciones de estudiantes y docentes para devengar la inversión que hace el estado Ecuatoriano en favor de los mismos.

FIRMAS DE LEGALIZACIÓN

FIRMADO Y SELLADO

EDGAR RUBEN LOPEZ OTAÑEZ
DOCENTE

LUIS ALBERTO GUERRA CRUZ
COORDINADOR DE AREA DE CONOCIMIENTO

LUCAS ROGERIO GARCES GUAYTA
DIRECTOR DE DEPARTAMENTO