SÍLABO DE ASIGNATURA

1. DATOS INFORMATIVOS

DEPARTAMENTO	CARRERA	NOMBRE ASIGNATURA	PERIODO ACADÉMICO	MODALIDAD	VIGENCIA DISEÑO
Ciencias de la Computación	Ingeniería en tecnologías de la información	ingeniería de la seguridad del software	202051	Presencial	

UNIDAD DE ORGANIZACIÓN CURRICULAR:			PRE-REQUISITOS	CÓDIGO	NRC
BÁSICA	PROFESIONAL	TITULACIÓN	Sistemas Operativos (COMPA0I12)	COMPA0I13	
	x				

NÚCLEOS BÁSICOS DE CONOCIMIENTO	CARGA HORARIA POR COMPONENTES DE APRENDIZAJE				SESIONES SEMANALES
	DOCENCIA	PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	APRENDIZAJE AUTÓNOMO	TOTAL	
• Fundamentos de seguridad informática • Mecanismos de seguridad • Aplicaciones de la seguridad de la información	32	32	32	96	2

CAMPO DE FORMACIÓN				
FUNDAMENT. TEÓRICA	PRAXIS PROFESIONAL	EPISTEMOLOGÍA Y METODOLOGÍA DE LA INVESTIGACIÓN	INTEGRACIÓN DE CONTEXTOS SABERES Y CULTURA	COMUNICACIÓN Y LENGUAJE
	X			
	Cátedra Integradora:	PPP:		
		X		

DOCENTE	NOMBRE COMPLETO	CORREO
Arturo de la Torre	César Arturo de la Torre Dávalos	cadelatorre@espe.edu.ec

FECHA ELABORACIÓN	FECHA DE ACTUALIZACIÓN	FECHA DE EJECUCIÓN
23/07/2020	23/07/2020	Noviembre 2020– Marzo 2021

DESCRIPCIÓN DE LA ASIGNATURA:

En esta asignatura, el estudiante aprenderá los principios fundamentales para implementar tecnologías de seguridad informática para garantizar el buen servicio de las aplicaciones y redes. Adicionalmente, el estudiante entenderá que existen muchas amenazas y vulnerabilidades que deben ser mitigadas, porque podrían permitir que existan atentados a los activos informáticos de las organizaciones. Finalmente, el estudiante aprenderá acerca de las soluciones tecnológicas para prevenir, detectar y recuperarse de los ataques.

CONTRIBUCIÓN DE LA ASIGNATURA / CONSTRUCTO A LOS RESULTADOS DE APRENDIZAJE DEL NIVEL:

La asignatura de ingeniería de la seguridad del software contribuye con los resultados de aprendizaje del nivel ya que proporciona al estudiante los conocimientos y destrezas para la selección, implementación y administración de sistemas y tecnologías necesarias para garantizar la seguridad de la información en reposo y en movimiento, así como también la confidencialidad, integridad y disponibilidad de las aplicaciones.

OBJETIVO GENERAL DE LA CARRERA :

La formación profesional del Ingeniero de Software estudia las fases del proceso de desarrollo de software (análisis, diseño, implementación, pruebas, implantación, retiro y gestión), con un enfoque sistémico y cuantificable, que integre los componentes teórico, metodológico y buenas prácticas

del desarrollo software; mediante la aplicación de: lenguajes de programación, métodos, técnicas, herramientas, normas y estándares; con el propósito de construir software de calidad que proporcione soluciones a las necesidades de los contextos de los diferentes sectores socio-económicos, productivos y tecnológicos.

RESULTADO DE APRENDIZAJE DEL NIVEL:

Identificar y analizar las necesidades de usuarios para la selección, implementación , evaluación, y administración de sistemas de seguridad informática que permitan minimizar las vulnerabilidades del software mediante la implementación de estrategias defensivas en contra de ciberatacantes.

RESULTADO DE APRENDIZAJE DE LA ASIGNATURA:

Conceptuales:
Conoce los asuntos e implicaciones éticas, teóricas y prácticas de seguridad de la información en sistemas de computación, bajo las políticas de seguridad, confidencialidad e integridad.

Procedimentales:
Maneja herramientas y modelos de control de acceso del sistema estándar, bajo políticas de seguridad, confidencialidad e integridad para evitar las vulnerabilidades de las redes computacionales.

Actitudinales:
Participa activamente en equipo en las discusiones sobre la seguridad de las aplicaciones de software.

PROYECTO INTEGRADOR:

PERFIL SUGERIDO DEL DOCENTE:

TÍTULO Y DENOMINACIÓN

GRADO: Ingeniero de Sistemas e Informática, Ingeniero en Computación, Ingeniero en Ciencias de la Computación, Ingeniero en Electrónica y afines.
POSGRADO: Maestría y/o Doctorado en Electrónica, Tecnologías de la Información, Ciencias de la Computación y afines.

1. SISTEMA DE CONTENIDOS, RESULTADOS Y ACTIVIDADES DE APRENDIZAJE

UC 1: FUNDAMENTOS DE SEGURIDAD INFORMÁTICA	
RESULTADO DE APRENDIZAJE DE LA UNIDAD: Al finalizar la unidad, el estudiante: • Entenderá los conceptos fundamentales que se requieren para implementar tecnologías en temas de seguridad informática. • Identificarán las amenazas y vulnerabilidades que están asociados a los servicios y aplicaciones informáticas. Entenderá los conceptos generales de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, no repudio, amenazas, vulnerabilidades, ataques, etc.)	
CONTENIDOS	**HORAS DE TRABAJO AUTÓNOMO**
1.1. Introducción a la seguridad 1.1.1. Fundamentos básicos de seguridad informática (concepto de seguridad informática, amenaza, vulnerabilidad, ataque y riesgo) 1.1.2 Principales herramientas tecnológicas para la seguridad informática. (Aseguramiento de los sistemas operativos, importancia del WAF, monitoreo de puertos y servicios, Antivirus, Firewall del Sistema Operativo, HIPS), 1.1.2. Objetivos de la seguridad (Confidencialidad, Integridad y Disponibilidad) 1..1.3 Herramientas tecnológicas para garantizar la confidencialidad, Integridad y Disponibilidad) 1.1.4. Requerimientos funcionales para implementar tecnologías de Seguridad Informática. 1.1.5 Análisis de las amenazas y vulnerabilidades mas comunes	**Prácticas de Aplicación y Experimentación** 1.1 Lectura de reportes de la industria de seguridad informática 1.2 Ejercicios acerca de seguridad tecnológica en el sistema operativo para prevenir ataques de SQL Injection. 1.3 Investigación bibliográfica sobre temas relacionados a la unidad.

ACTIVIDADES DE APRENDIZAJE / HORAS CLASE	
COMPONENTE DE DOCENCIA	**16**
PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	**8**
HORAS DE TRABAJO AUTÓNOMO	**8**
TOTAL DE HORAS POR UNIDAD	32/96

UC 2: MECANISMOS DE SEGURIDAD	
Al finalizar la unidad, el estudiante • Conocer los elementos tecnológicos más importantes para la seguridad de las aplicaciones y los servicios de las redes de datos. • Entender los fundamentos básicos para las implementaciones de sistemas seguros. • Comprender las tendencias actuales del campo de la seguridad • Entender y aplicarán los algoritmos y soluciones criptográficos más populares.	
CONTENIDOS	**HORAS DE TRABAJO AUTÓNOMO**

2.1. Seguridad para los servicios en la Red 2.1.1. Conceptos generales de ciberseguridad. 2.1.2. Aplicar los elementos más comunes de tecnologías para la ciberseguridad. 2.1.3 Gestión de servicios y tareas 2.1.4 NEXT GENERATION FIREWALLS 2.1.5 IDS / IPS / HIPS 2.1.6 Protección de las aplicaciones en Internet, limitar la acción de robots y buscadores. **2.2. Fundamentos de criptografía** 2.2.1. Conceptos generales 2.2.2. Funciones hash, MD5, aplicados al software y la información de los usuarios. 2.2.3. Encriptación simétrica y asimétrica 2.2.4. Firmas digitales, certificados digitales 2.2.5. Importancia y aplicación de los PKIs **2.3. Temas actuales de seguridad** 3.2.1 Blockchain 3.2.2 Seguridad cognitiva 3.2.3 Seguridad para cloud 3.2.4 Seguridad de IoT	**Prácticas de Aplicación y Experimentación** **1.1** Investigación de nuevas tendencias de soluciones de seguridad **1.2** Ejercicios sobre los temas de la unidad.

ACTIVIDADES DE APRENDIZAJE / HORAS CLASE	
COMPONENTE DE DOCENCIA	**16**
PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	**8**
HORAS DE TRABAJO AUTÓNOMO	**8**
TOTAL DE HORAS POR UNIDAD	32/96

UC 3: APLICACIONES DE LA SEGURIDAD DE LA INFORMACIÓN

RESULTADO DE APRENDIZAJE DE LA UNIDAD:

Al finalizar la unidad el estudiante:

- Identificará los diferentes factores que intervienen en los procesos de autenticación de usuarios
- Entenderá los servicios mas modernos utilizados para la autenticación de usuarios
- Comprenderá las diferencias entre los modelos y tipos de control de accesos
- Comprenderá la importancia de implementar protocolos criptográficos para la información en reposo y la información en movimiento.

CONTENIDOS (correspondencia con el Diseño curricular)	**HORAS DE TRABAJO AUTÓNOMO**
3.1. Importancia de la autenticación de usuarios para los servicios y aplicaciones. 3.1.1. Factores de autenticación 3.1.2 Perfiles de usuarios **3.2. Control de Acceso** 3.2.1. Modelos de control de acceso a las aplicaciones y servicios BLP vs Biba 3.2.2. Tipos de control de acceso (DAC, MAC) **3.3. Seguridad Física** 3.3.1 El modelo de seguridad de Google. **3.4. Protocolos criptográficos y sistemas de autenticación** 3.4.1. Evolución de los protocolos criptográficos 3.4.2. TLS/SSL y tecnologías de VPN	**Prácticas de Aplicación y Experimentación** **1.1** Estudio de casos prácticos de autenticación y control de acceso **1.2** Ejercicios de aplicación de protocolos criptográficos y generación de soluciones **1.3** Investigación bibliográfica sobre temas relacionados a la unidad

3.4.2. Kerberos, Single Sign On	

COMPONENTES APRENDIZAJE / HORAS CLASE	
COMPONENTE DE DOCENCIA	16
PRÁCTICAS DE APLICACIÓN Y EXPERIMENTACIÓN	8
HORAS DE TRABAJO AUTÓNOMO	8
TOTAL DE HORAS POR UNIDAD	32/96

SUMA TOTAL POR UNIDADES				
COMPONENTES DE APRENDIZAJE	C.D	C.P	A.A.	TOTAL
UNIDAD I	16	8	8	32
UNIDAD II	16	8	8	32
UNIDAD III	16	8	8	32
SUBTOTAL POR COMPONENTE	48	24	24	96

2 APORTE DE LA ASIGNATURA AL PROYECTO INTEGRADOR

PROYECTO INTEGRADOR DEL NIVEL	SOLUCIONES TECNOLÓGICAS PARA PREVENIR, DETECTAR Y RECUPERARSE DE ATAQUES INFORMÁTICOS			
RESULTADO DE APRENDIZAJE POR UNIDAD CURRICULAR	ACTIVIDADES INTEGRADORAS	NIVELES DE LOGRO		
		A Alto	B Medio	C Baja
Utiliza la tecnología para cerrar las brechas de seguridad en los sistemas informáticos.	Comprensión y conocimiento de las diferentes formas operación de los sistemas.	x		
Conoce las herramientas tecnológicas que se utilizan para garantizar la seguridad de los datos en movimiento	Implementación de tecnologías de seguridad para garantizar integridad, confidencialidad y disponibilidad.	x		
Gestiona los diferentes niveles de seguridad que requieren los usuarios de un sistema informático.	Aporta con los diferentes perfiles que garantizan la seguridad de los datos en reposo.			

3 PROYECCIÓN METODOLÓGICA Y ORGANIZATIVA PARA EL DESARROLLO DE LA ASIGNATURA

MÉTODOS DE ENSEÑANZA – APRENDIZAJE

Se emplearán variados métodos de enseñanza para generar un aprendizaje de constante actividad, para lo que se propone la siguiente estructura:
1Talleres
2 Clase Magistral
3 Estudio de Casos
4 Resolución de Problemas

La evaluación cumplirá con las tres fases: diagnóstica, formativa y sumativa, valorando el desarrollo del estudiante en cada tarea y en especial en las evidencias del aprendizaje de cada unidad.

PROYECCIÓN DEL EMPLEO DE LAS TICS EN LOS PROCESOS DE APRENDIZAJE:

1 Herramientas Colaborativas (Google, Drive, OneDrive, otros)
2 Material Multimedia
3 Aula Virtual

4 TÉCNICAS Y PONDERACIÓN DE LA EVALUACIÓN

Técnica de evaluación	1er Parcial*	2do Parcial*	3er Parcial*
Resolución de ejercicios	1	1	1
Investigación Bibliográfica			
Pruebas orales/escrita	1	1	1
Laboratorios			
Talleres	3	3	3
Prácticas	2	2	2
Exposición			
Trabajo colaborativo	5	5	5
Examen parcial	6	6	6
Portafolio			
Otras formas de evaluación	**2**	**2**	2
Total:	**20**	**20**	**20**

5 BIBLIOGRAFÍA BÁSICA/ TEXTO GUÍA DE LA ASIGNATURA

TITULO	AUTOR	EDICIÓN	AÑO	IDIOMA	EDITORIAL
CISSP All-in-One Exam Guide	Harris, S., Maymi, F	8	2018	Inglés	McGraw Hill
Network Security Essentials	Stallings, W.	6	2016	Inglés	Prentice-Hall
CIBERSEGURIDAD	Alejandro Corletti Estrada	2	2017	Español	DARFE

6 BIBLIOGRAFÍA COMPLEMENTARIA

TITULO	AUTOR	EDICIÓN	AÑO	IDIOMA	EDITORIAL
GUIA DE IMPLANTACION DE SGSI	**AUDISEC**	**3**	**2010**	**ESPAÑOL**	**SGSI**

7 LECTURAS PRINCIPALES

TEMA	TEXTO	PÁGINA
Tipos de ataques e intrusos en las redes informáticas	Álvaro Gómez Vieites	
Modelo Para Seguridad de la Información en TIC	Jorge Burgos Salazar, Pedro G. Campos	
Seguridad de redes	Network Security Essentials	

8 ACUERDOS CON LOS ESTUDIANTES

DEL DOCENTE:

- Integridad: honestidad, veracidad, imparcialidad, respeto, responsabilidad.
- Se exigirá puntualidad, no se permitirá el ingreso de los estudiantes con retraso.
- La copia de exámenes, pruebas, informes, capítulos, ensayos, entre otros, será severamente corregida, inclusive podría ser motivo de la pérdida automática del semestre, (código de ética de la universidad).
- Respeto en las relaciones docente – alumno y alumno – alumno será exigido en todo momento, esto será de gran importancia en el desarrollo de las discusiones en clase.

DE LOS ESTUDIANTES:

- Acatar y cumplir las consignas académicas, tecnológicas y administrativas.
- Cumplir los tiempos de entrega y/o presentación de actividades y tareas de aprendizaje.
- Desarrollar conscientemente la honestidad y deberán manifestar a través de sus actitudes.
- Deberán demostrar siempre respeto en sus actitudes.

9 FIRMAS DE LEGALIZACIÓN

Ing. Arturo de la Torre, MSc.
DOCENTE

Ing. Diego Marcillo, PhD
COORDINADOR CAMPO DE CONOCIMIENTO

Ing. Mauricio Campaña
DIRECTOR DE LA CARRERA DE INGENIERÍA EN SOFTWARE