SÍLABO

FACULTAD DE INGENIERÍA

SEPTIEMBRE 2023-FEBRERO 2024

NOMBRE DE LA ASIGNATURA	CÓDIGO:	17942

SEGURIDAD INFORMÁTICA - GRUPO: 1			
CARRERA	COMPUTACION REDISEÑO		
CICLO O SEMESTRE	SEPTIMO NIVEL	**EJE DE FORMACIÓN**	PROFESIONALES, PRAXIS PROFESIONAL
CRÉDITOS DE LA ASIGNATURA	3	**MODALIDAD:**	PRESENCIAL

CARGA HORARIA

COMPONENTES DEL APRENDIZAJE	Horas / Semana	Horas / Periodo Académico
APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	4.0	64.0
APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	2.0	32.0
APRENDIZAJE AUTÓNOMO (AA)	3.0	48.0
Total Horas:	9.0	144.0

PROFESOR(ES) RESPONSABLE(S):

PONCE VASQUEZ DIEGO ARTURO - (D.P.)	(diego.ponce@ucuenca.edu.ec)	PRINCIPAL

DESCRIPCIÓN DE LA ASIGNATURA:

Resumen descriptivo en torno al propósito, la estrategia metodológica y el contenido fundamental de la asignatura.

La asignatura de seguridad de la información introduce al estudiante a los conceptos, técnicas, mecanismos y diseño de la seguridad en un entorno informático.
Para cumplir con este objetivo se hace una revisión de los diferentes conceptos de seguridad de los sistemas informáticos tales como: vulnerabilidades, amenazas, riesgos, ataques y su prevención y respuesta. Se abordan los principios de defensa, políticas de seguridad, algoritmos, protocolos, mecanismos, diseño de sistemas de seguridad, se introduce al estudiante a las normas, estándares y recomendaciones existentes (mejores prácticas ISO, NIST, ISACA, CISCO TAC, NSA, OWASP y otros).

Se rquiere conocer las asignaturas de redes de computadores y sistemas distribuidos.

REQUISITOS DE LA ASIGNATURA

Esta asignatura no tiene co-requisitos

PRE-REQUISITOS	
Asignatura	**Código**
ORGANIZACIÓN Y ARQUITECTURA DE COMPUTADORES	18586
LENGUAJES DE PROGRAMACIÓN	18585

OBJETIVO(S) DE LA ASIGNATURA:

Objetivos general y específicos de la asignatura en relación al Perfil de salida de la carrera.

Objetivo general: Adquirir los conocimientos y ser capaces de aplicar el diseño y los principales mecanismos de seguridad en los sistemas informáticos.

Objetivos específicos:

1. Comprende los fundamentos de los algoritmos y mecanismos de seguridad informática.

2. Conoce las mejores prácticas de diseño para garantizar la seguridad suficientemente buena de un sistema informático.

3. Conoce los estándares y recomendaciones de diseño vigentes.

4. Conoce el funcionamiento y uso de los algoritmos de seguridad, los protocolos de sguridad y su aplicación.

LOGRO DE LOS RESULTADOS DE APRENDIZAJE, INDICADOR(ES) Y ESTRATEGIA(S) DE EVALUACIÓN

Resultados o Logros de Aprendizaje (RdA's) de la Unidad de Organización Curricular (UOC) correspondiente, Indicadores y Estrategias de Evaluación de la Asignatura, tomando como referencia el Perfil de salida (PdS) y la Organización Curricular (OC) del Proyecto de Carrera (PdC).

RESULTADOS O LOGROS DE APRENDIZAJE	INDICADORES	ESTRATEGIAS DE EVALUACIÓN
RdA1. Conceptualiza los riesgos de un sistema informático y es capaz de proponer los mecanismos para garantizar la seguridad informática en sus aspectos fundamentales.	• Realiza el diagnóstico de la situación actual de una red o sistema informático. • Identifica los requerimientos de seguridad a garantizar.	• TRABAJO: ANALIZAR LA TOPOLOGIA DE UNA RED Y PROPONER UN DISEÑO DE SEGURIDAD CON LOS MECANISMOS DE PROTECCION SUFICIENTEMENTE BUENA. • TRABAJO: BUSQUEDA BIBLIOGRAFICA DE LOS ESTANDARES NIST SP 800 Y SP 1800, WWW.NIST.GOV, PARA ANALIZAR LA SEGURIDAD DE SUSTEMAS INFORMATICOS DE DIFERENTE TIPO.
RdA2. Determina y usa buenas prácticas en el diseño y desarrollo de la seguridad informática, puede realizar las pruebas y documentar las recomendaciones de seguridad a ser adoptadas por el personal de informática y los usuarios del sistema a proteger.	• Expone las buenas prácticas de diseño de software. • Realiza ejemplos de problemas reales de diseño de seguridad. • Utiliza en la práctica las técnicas y metodologías aprendidas.	• TRABAJO: REVISAR EL DISEÑO DE SEGURIDAD CONSIDERANDO LAS RECOMENDACIONES, EN CUANTO A LOS DIFERENTES ASPECTOS DE HARDWARE Y SOFTWARE. • PRUEBA: PRINCIPIOS DE SEGURIDAD, VULNERABILIDADES Y MECANISMOS DE PROTECCION.
RdA3. Determina y usa herramientas para la implementación de la seguridad de un sistema informático, sus componentes y pruebas funcionales.	• Conoce y aplica las normas y recomendaciones ISO, Owasp, IETF, NIST y de fabricantes en el contexto pertinente.	• TRABAJO: APLICAR LAS NORMAS DE SEGURIDAD ISO 27000 E ISO 31000.
RdA4. Determina y usa herramientas de seguridad.	• Expone diferentes alternativas a utilizar dependiendo de la tecnología. • Explica pruebas aplicadas a un esquema de seguridad determinado. • Expone conceptualmente los mecanismos de seguridad.	• TRABAJO: PROTECCION DE SISTEMAS INFORMATICOS EN ENTORNOS CLIENTE-SERVIDOR, INTERNET, IoT, cLOUD Y MÓVIL CELULAR. • PRUEBA: ALGORITMOS Y PROTOCOLOS CRIPTOGRAFICOS.

CONTENIDOS, SESIONES Y ACTIVIDADES DE APRENDIZAJE

Título de la Unidad, sub -unidades, nro. de sesión y actividades para los componentes de aprendizaje.

SUB-UNIDADES	Nro. SESIÓN	COMPONENTE DE APRENDIZAJE	ACTIVIDADES DE APRENDIZAJE
1. PARTE I: PRINCIPIOS Y TECNOLOGÍA DE LA SEGURIDAD INFORMÁTICA.			

SUB-UNIDADES	Nro. SESIÓN	COMPONENTE DE APRENDIZAJE	ACTIVIDADES DE APRENDIZAJE	
1. Introducción y Herramientas. 2. Autentificación de usuarios. 3. Control de acceso. 4. Seguridad de bases de datos y en la nube. 5. Software malicioso. 6. Ataques de denegación de servicio. 7. Detección de Intrusiones. 8. Cortafuegos.	1	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: PRESENTACION DEL SILABO, INTRODUCCION A LA SEGURIDAD INFORMATICA.	2 horas
	2	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: GENERALIDADES	4 horas
	3	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: HERRAMIENTAS DE SEGURIDAD	2 horas
	4	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: AUTENTIFICACION DE USUARIOS	2 horas
	5	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: CONTROL DE ACCESO.	2 horas
	6	APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	TALLER: AAA, Open Radius y Tacacs de Cisco.	6 horas
	7	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: SEGURIDAD EN BASES DE DATOS Y EN LA NUBE.	2 horas
	8	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: SOFTWARE MALICIOSO, MALWARE.	2 horas
	9	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: ATAQUES DE DENEGACION DE SERVICIO.	2 horas
	10	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: DETECCION DE	2 horas
	11	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: CORTAFUEGOS Y SISTEMAS DE PREVENCION DE	4 horas
	12	APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	TALLER: DISEÑO DE LA SEGURIDAD DE REDES.	6 horas
		APRENDIZAJE AUTÓNOMO (AA)	TRABAJO: BUSQUEDA BIBLIOGRAFICA DE PRINCIPIOS DE LA SEGURIDAD EN SISTEMAS DE TI.	2 horas
	13	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: ATAQUE DE DESBORDAMIENTO DE PILA.	2 horas
2. PARTE II: SEGURIDAD DEL SOFTWARE Y SISTEMAS DE CONFIANZA.				
1. Desbordamiento de Pila y sus consecuencias 2. Seguridad del software 3. Seguridad del Sistema Operativo 4. Seguridad Multinivel 5. Computación de confianza	14	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: SEGURIDAD DEL	4 horas
	15	APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	TALLER: OWASP	6 horas
	16	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: SEGURIDAD DE SISTEMAS OPERATIVOS	2 horas
	17	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: COMPUTACION DE CONFIANMZA Y SEGURIDAD MULTINIVEL	2 horas
		APRENDIZAJE AUTÓNOMO (AA)	TRABAJO: DISEÑO DE LA SEGURIDAD DE REDES.	8 horas

SUB-UNIDADES	Nro. SESIÓN	COMPONENTE DE APRENDIZAJE	ACTIVIDADES DE APRENDIZAJE	
3. PARTE III: GESTIÓN DE LA SEGURIDAD.				
1. Diagnóstico y Gestión de la seguridad 2. Planificación, Control y procedimientos 3. Seguridad física y de infraestructura 4. Seguridad del recurso humano 5. Auditoria de seguridad 6. Aspectos éticos y legales	18	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: GESTION DE LA SEGURIDAD Y DIAGNOSTICO DEL CLASE: CONTROLES PLANES Y PROCEDIMIENTOS DE SEGURIDAD.	2 horas 2 horas
	19	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: SEGURIDAD FISICA Y DE INFRAESTRUCTURA DE TI. CLASE: SEGURIDAD DEL RECURSOS HUMANO.	2 horas 2 horas
	20	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: AUDITORIA DE SEGURIDAD. CLASE: NORMA NIST SP.	2 horas 2 horas
	21	APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	TALLER: NORMAS NIST SP 800 Y SP 1800.	6 horas
		APRENDIZAJE AUTÓNOMO (AA)	TRABAJO: REDISEÑO DE SEGURIDAD UTILIZANDO LA NORMA NIST SP 800 Y SP 1800.	12 horas
	22	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: ASPECTOS ETICOS Y LEGALES.	2 horas
		APRENDIZAJE AUTÓNOMO (AA)	PRUEBA: FUNDAMENTOS Y GESTION DE SEGURIDAD.	2 horas
4. PARTE IV: ALGORITMOS CRIPTOGRÁFICOS.				
1. Criptografía simétrica 2. Criptografía de clave pública	23	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: CIFRADO SIMETRICO Y CONFIDENCIALIDAD DE LOS MENSAJES. CLASE: CRIPTOGRAFIA DE CLAVE PUBLICA Y AUTENTIFICACION DE LOS MENSAJES.	3 horas 3 horas
	24	APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	TALLER: APLICACION DE LAS NORMAS ISO.	4 horas
		APRENDIZAJE AUTÓNOMO (AA)	TRABAJO: NORMAS ISO 27000, 31000 Y 37000. PRUEBA: ALGORITMOS Y PROTOCLOS CRIPTOGRAFICOS.	14 horas 2 horas
5. PARTE V: SEGURIDAD DE REDES.				

SUB-UNIDADES	Nro. SESIÓN	COMPONENTE DE APRENDIZAJE	ACTIVIDADES DE APRENDIZAJE	
1. Protocolos y Estándares de Internet 2. Autentificación 3. Seguridad en Redes Inalámbricas 4. Seguridad en redes IoT 5. Seguridad en entornos Cloud. 6. Seguridad en entornos móviles celulares.	25	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: PROTOCOLOS Y ESTANDARES DE SEGURIDAD.	2 horas
	26	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: AUTENTIFICACION EN INTERNET.	2 horas
	27	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: SEGURIDAD EN REDES INALAMBRICAS. CLASE: SEGURIDAD EN ENTORNOS IoT.	2 horas 2 horas
	28	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	CLASE: SEGURIDAD EN ENTORNOS MOVILES CELULARES.	2 horas
	29	APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	TALLER: PROTECCION DE SISTEMAS DE INFORMACION EN DIFERENTES ENTORNOS.	4 horas
	30	APRENDIZAJE AUTÓNOMO (AA)	TRABAJO: DISEÑO DE LA SEGURIDAD EN DIFERENTES ENTORNOS DE RED.	8 horas

APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	64 horas
APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	32 horas
APRENDIZAJE AUTÓNOMO (AA)	48 horas
Total Planificación:	144 horas

RECURSOS O MEDIOS PARA EL APRENDIZAJE

Equipos, materiales, instrumentos tecnológicos, reactivos, entre otros, que serán utilizados durante el desarrollo de la asignatura.

• Aula, laboratorio de cómputo, proyector digital, software libre, información en internet, bibliografia y artículos especializados, videoconferencia y simuladorres.

CRITERIOS PARA LA ACREDITACIÓN DE LA ASIGNATURA

Parámetros de acreditación, tomando como referencia los Resultados de Aprendizaje (RdA's), indicadores y criterios de evaluación planteados y en base a la normativa de evaluación y calificaciones vigente en la Universidad de Cuenca y Consejo de Educación Superior (CES).

CRITERIO GENERAL DE ACREDITACIÓN	PUNTAJE
TRABAJOS	20
PRUEBAS	20
TALLERES	10
EXAMENES	50
TOTAL:	100

	DETALLE DE CRITERIOS DE ACREDITACIÓN	PUNTAJE / CRITERIO GENERAL	
C94	APROVECHAMIENTO I		
	TRABAJO 1: DISEÑO DE SEGURIDAD	5	TRABAJOS
	TRABAJO 2: ESTANDARES DE SEGUREIDAD.	5	TRABAJOS
	PRUEBA 1: PRINCIPIOS DE SEGURIDAD, VULNERABILIDADES Y MECANISMOS DE PROTECCION.	10	PRUEBAS
	TALLER 1: DISEÑO DE SEGURIDAD	5	TALLERES

	DETALLE DE CRITERIOS DE ACREDITACIÓN	PUNTAJE / CRITERIO GENERAL	
C95	INTERCICLO		
	EXAMEN INTERCICLO	20	EXAMENES
C96	APROVECHAMIENTO II		
	TRABAJO 3: NORMAS ISO.	5	TRABAJOS
	TRABAJO 4: PROTECCION DE SISTEMAS INFORMATICOS EN ENTORNOS ESPECIFICOS.	5	TRABAJOS
	PRUEBA 2: ALGORITMOS CRIPTOGRAFICOS Y PROTOCOLOS DE SEGURIDAD EN TCP-IP.	10	PRUEBAS
	TALLER 2: ANALISIS DE VULNERABILIDADES CON KALI LINUX	5	TALLERES
C97	FINAL		
	EXAMEN FINAL	30	EXAMENES
C98	SUSPENSIÓN		
	Total:	100	

TEXTOS U OTRAS REFERENCIAS REQUERIDAS PARA EL APRENDIZAJE DE LA ASIGNATURA

Libros, revistas, bases digitales, periódicos, direcciones de Internet y demás fuentes de información, pertinentes y actuales.

BÁSICA

1. William Stallings y Lawrie Brown, Computer Security, Pearson, (2015). Compatible con recomendación ACM/IEEE CS'2013.
2. Gómez Vieites Álvaro, Enciclopedia de la Seguridad Informática, Editorial RAMA, edición, ISBN: 9788478977314.
3. David Kim, Michael Solomon (2018), Fundamentals of Information System Security, Jonnes & Barllett Learning, third edition, ISBN 9781284116458.
4. Bressoud David, (1994). Factorization and Primality Testing, Springer.

COMPLEMENTARIA

1. Stallings William, Network Security Essentials, Application and standards, Fifth Edition, Prentice Hall, ISBN-13: 978-0-13-238033-1.
2. Mericke Kiaeo, Diseño de la Seguridad en Redes, Academia Cisco, Pearson Editorial ISBN: ISBN 9788420534640.
3. Recomendaciones ISO 27000, 31000, 37000 Industrial Standard Organization, www.iso.org.
4. NIST, www.nist.gov, estandares FIPS, SP800, SP1800.

Docente: PONCE VASQUEZ DIEGO ARTURO

Director: VEINTIMILLA REYES JAIME EDUARDO

Finalizado: 13/9/2023

Publicado: 7/10/2023