UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
ESCUELA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

1. Datos generales

Materia: SEGURIDAD DE LA INFORMACIÓN
Código: ICC0032
Paralelo: A
Periodo : Marzo-2023 a Julio-2023
Profesor: CRESPO MARTINEZ PAUL ESTEBAN
Correo electrónico: ecrespo@uazuay.edu.ec

Nivel: 6

Distribución de horas.

Docencia	Práctico	Autónomo: 56		Total horas
		Sistemas de tutorías	Autónomo	
48	16		56	120

Prerrequisitos:

Código: ICC0025 Materia: REDES I

2. Descripción y objetivos de la materia

Esta materia cubre por medio de la transferencia de conocimiento magistral, combinado con practica e investigación temas relevantes de seguridad de la información como son los principios básicos de la seguridad informática, el sistema de gestión de seguridad de la información, aspectos legales de la seguridad informática, ataques informáticos, técnicas de hackeo más frecuentes, análisis forense y respuesta a incidentes de seguridad y planes para la continuidad.

Es pieza fundamental del currículum del Ingeniero en Ciencias de la Computación ya que permite gestionar a la Seguridad de la Información velando por el triángulo de confidencialidad, integridad y disponibilidad de la información para que sea gestionado de la mejor forma basado en buenas prácticas internacionales.

Las nuevas de tecnologías de información promueven a las empresas a utilizar estas tecnologías. Esto crea una dependencia del uso de TI, así como la vulnerabilidad a posibles riesgos en la gestión de la información. Esta materia da a conocer por medio de la transferencia de conocimiento magistral, combinado con practica e investigación en la aplicación de los métodos, técnicas y herramientas de Seguridad de la Información. Permitiendo analizar, diseñar, implementar y gestionar sistemas de seguridad de la Información aplicando estándares internacionales. Así como se acciona la investigación, conocer, analizar y determinar los mecanismos de ataque y respuesta a incidentes informáticos. La asignatura se alinea con el ODS 4: Educación de calidad, puesto que se plantean realizar webinars sobre temáticas de ciberseguridad, los cuales consisten clases demostrativas abiertas a la comunidad. En ayudantías de cátedra para los laboratorios se considerará primordialmente a las estudiantes mujeres, con el objetivo de contribuir con el ODS5: Igualdad de género.

3. Objetivos de Desarrollo Sostenible

4. Contenidos

1.1	Vulnerabilidades, ataques e importancia de la seguridad. Importancia de la seguridad
1.2	Principios de la seguridad informática
1.3	Elementos de seguridad. El Triángulo de la Seguridad, Funcionalidad y Facilidad de uso
1.4	Revisión de las ISO 27001, ISO 27002, ISO 27005.

1.5	Políticas de seguridad. Aspectos organizativos de la seguridad de la información. Seguridad ligada a los recursos humanos
1.6	Gestión de activos
1.7	Control de accesos
1.8	Cifrado
1.9	Seguridad física y ambiental, operativa y en telecomunicaciones
1.10	Adquisición, desarrollo y mantenimiento de los sistemas de información. Proveedores. Gestión de incidentes en la seguridad de la información
1.11	Gestión de la continuidad del negocio
1.12	Cumplimiento
1.13	Práctica
2.1	SGSI - Sistema de Gestión de Seguridad de la Información
2.2	PDCA - Modelo para establecer, implementar, monitorear y mejorar el SGSI
2.3	Aspectos legales de la seguridad informática
2.4	Firma electrónica
2.5	Practica
3.1	Caracterización de los hackers
3.2	Fases de un ataque
4.1	Reconocimiento y escaneo (técnicas y herramientas)
4.2	Ataque (obtener acceso) y mantener el acceso (técnicas y herramientas)
4.3	Eliminación del rastro (técnicas y herramientas). Herramientas varias de hackeo

5. Sistema de Evaluación

Resultado de aprendizaje de la carrera relacionados con la materia

Resultado de aprendizaje de la materia	Evidencias
bb. Utiliza los fundamentos y mejores prácticas de la industria de la seguridad de la Información para desarrollar, integrar y gestionar políticas, técnicas y mecanismos de seguridad.	
-Diseña, implementa, analiza y gestiona sistemas de seguridad de la Información aplicando estándares internacionales	-Prácticas de laboratorio -Reactivos
-Investiga, conoce, analiza y determina los mecanismos de ataque y respuesta a incidentes informático	-Prácticas de laboratorio -Reactivos

Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Prácticas de laboratorio	Prácticas de laboratorio	Principios básicos de la seguridad informática, Sistema de Gestión de Seguridad de la Información	APORTE	5	Semana: 4 (03-ABR-23 al 06-ABR-23)
Reactivos	Prueba con reactivos	Principios básicos de la seguridad informática, Sistema de Gestión de Seguridad de la Información	APORTE	5	Semana: 4 (03-ABR-23 al 06-ABR-23)
Prácticas de laboratorio	prácticas de laboratorio	Ataque Informático, Técnicas de Hackeo	APORTE	5	Semana: 10 (15-MAY-23 al 20-MAY-23)
Reactivos	Prueba con reactivos	Ataque Informático, Técnicas de Hackeo	APORTE	5	Semana: 10 (15-MAY-23 al 20-MAY-23)
Prácticas de laboratorio	Prácticas de laboratorio	Análisis forense, Respuesta a incidentes de seguridad y planes para la continuidad del negocio	APORTE	5	Semana: 14 (12-JUN-23 al 17-JUN-23)
Reactivos	Prueba con reactivos	Análisis forense, Respuesta a incidentes de seguridad y planes para la continuidad del negocio	APORTE	5	Semana: 19-20 (16-07-2023 al 22-07-2023)
Prácticas de laboratorio	trabajo de investigación	Análisis forense, Ataque Informático, Principios básicos de la seguridad informática, Respuesta a incidentes de seguridad y planes para la continuidad del negocio, Sistema de Gestión de Seguridad de la Información, Técnicas de Hackeo	EXAMEN	10	Semana: 19-20 (16-07-2023 al 22-07-2023)
Reactivos	examen con reactivos	Análisis forense, Ataque Informático, Principios básicos de la seguridad informática, Respuesta a incidentes de seguridad y planes para la continuidad del negocio, Sistema de Gestión de Seguridad de la Información, Técnicas de Hackeo	EXAMEN	10	Semana: 19-20 (16-07-2023 al 22-07-2023)
Reactivos	el examen consiste en un ejercicio práctico y preguntas de opción múltiple	Análisis forense, Ataque Informático, Principios básicos de la seguridad informática, Respuesta a incidentes de seguridad y planes para la continuidad del negocio, Sistema de Gestión de Seguridad de la Información, Técnicas de Hackeo	SUPLETORIO	20	Semana: 19 (al)

Metodología

Descripción	Tipo horas
El estudiante deberá revisar el material que se entregue previo a la clase. En clase se despejarán las dudas que se presenten por parte de los estudiantes, a manera de hacer la clase más participativa	Autónomo
En clase, se repasará la teoría y aspectos de la asignatura para realizar prácticas de laboratorio. Se hará uso de simuladores, máquinas virtuales y una guía de prácticas con el objetivo de realizar las prácticas de laboratorio. Al final, el estudiante deberá realizar un informe de las prácticas realizadas según las instrucciones del profesor. Al final de cada trabajo se incluirá la leyenda: "por ética y por mi honor declaro que este trabajo es fruto de mi propio esfuerzo"	Total docencia

Criterios de evaluación

Descripción	Tipo horas
Las tareas enviadas a realizar de forma autónoma (prácticas de laboratorio en casa) serán consideradas como parte del aporte "Prácticas de laboratorio" del componente docente.	Autónomo
Los aportes son calificados en dos instancias: 1. Pruebas en base de reactivos, relacionados con el material de lectura y teoría relacionada con la ciberseguridad 2. Prácticas de laboratorio que serán realizadas en clase No se receptarán trabajos de forma extratemporánea. Todos los trabajos deberán ser cargados en el aula virtual Los trabajos serán revisados por un control de similitud. Trabajos copiados entre compañeros, de internet o de cualquier otra fuente será calificado automáticamente con 0 puntos y aplicado lo que dictamina el reglamento universitario.	Total docencia

6. Referencias

Bibliografía base

Libros

Autor	Editorial	Título	Año	ISBN
ISO		ISO/IEC 27001:2013	2013	
ISO		ISO/IEC 27002:2013	2013	
ISO		ISO/IEC 27005:2018	2018	
OWASP		OWASP top 10 – 2017	2017	
Crespo Martínez, Esteban; Orellana Cordero, Marcos		Metodología para la gestión de Riesgos de Información en MPYMES	2019	
Mitnick Kevin; Simon, William		The art of deception	2014	
Weidman, Georgia		Penetration Testing, A hands-on introduction to hacking	2014	
Stuttard, Dafydd; Pinto, Marcus		The web application hacker's handbook		
Gómez, Alberto		Enciclopedia de la seguridad informática	2011	

Web

Autor	Título	Url
ISO	ISO27000	http://www.iso27000.es
OWASP	OWASP	https://www.owasp.org

Software

Revista

Bibliografía de apoyo

Libros

Web

Software

Revista

Docente

Director/Junta

Fecha aprobación: 08/03/2023

Estado: Aprobado