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-2024 a Junio-2024
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	Principios básicos de la seguridad informática
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	Sistema de Gestión de Seguridad de la Información
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	Ataque Informático
3.1	Caracterización de los hackers
3.2	Fases de un ataque
4	Técnicas de Hackeo
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	Análisis forense
5.1	Introducción al análisis forense y el principio de Lockard. Herramientas y técnicas para recolección, tratamiento, almacenamiento y análisis de evidencias
5.2	Ejercicios de análisis forense
6	Respuesta a incidentes de seguridad y planes para la continuidad del negocio
6.1	Respuesta a incidencias de seguridad de la información.

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	-Evaluación escrita -Investigaciones -Prácticas de laboratorio -Reactivos -Trabajos prácticos - productos
-Investiga, conoce, analiza y determina los mecanismos de ataque y respuesta a incidentes informático	-Evaluación escrita -Investigaciones -Prácticas de laboratorio -Reactivos -Trabajos prácticos - productos

Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Trabajos prácticos - productos	Trabajo sobre identificación de los activos de información y cálculo de riesgo	Principios básicos de la seguridad informática	APORTE	4	Semana: 2 (04-MAR-24 al 09-MAR-24)
Evaluación escrita	prueba sobre fundamentos de ciberseguridad	Principios básicos de la seguridad informática, Sistema de Gestión de Seguridad de la Información	APORTE	4	Semana: 3 (11-MAR-24 al 16-MAR-24)
Investigaciones	Investigación: Tendencias en la ciberseguridad en la sociedad y las empresas	Principios básicos de la seguridad informática, Sistema de Gestión de Seguridad de la Información	APORTE	2	Semana: 4 (18-MAR-24 al 23-MAR-24)
Trabajos prácticos - productos	informe de prácticas de laboratorio sobre reconocimiento y escaneo	Ataque Informático, Técnicas de Hackeo	APORTE	5	Semana: 6 (01-ABR-24 al 06-ABR-24)
Prácticas de laboratorio	Informe de prácticas de laboratorio sobre ataques	Ataque Informático, Técnicas de Hackeo	APORTE	5	Semana: 7 (08-ABR-24 al 13-ABR-24)
Trabajos prácticos - productos	Informe de práctica de laboratorio en formato IEEE. Evaluación forense.	Análisis forense	APORTE	5	Semana: 12 (13-MAY-24 al 18-MAY-24)
Trabajos prácticos - productos	informe de prácticas sobre técnicas de ataque	Análisis forense, Técnicas de Hackeo	APORTE	5	Semana: 12 (13-MAY-24 al 18-MAY-24)
Trabajos prácticos - productos	Capítulo de libro sobre técnicas de ataque y contramedidas de seguridad. Guía de aseguramiento.	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	20	Semana: 17-18 (16-06-2024 al 29-06-2024)
Reactivos	Examen supletorio basado en 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: 19-20 (al)

Metodología

Descripción	Tipo horas
El estudiante deberá realizar las actividades que se presenten en el aula virtual. Esto implica cursos adicionales y prácticas en simuladores creados para fortalecer el conocimiento.	Autónomo
La clase será impartida con clases magistrales y prácticas de laboratorio. Es importante que el estudiante revise el material y profundice los temas para debatirlos en clase. Si ha revisado este sílabo completamente, envíe un correo a ecrespo@uazuay.edu.ec con sus nombres completos y su código de estudiante, indicando las fechas en las que se realizarán las actividades. Se espera este correo durante la primera semana de clase. No se receptarán trabajos o evaluaciones fuera de tiempo.	Total docencia

Criterios de evaluación

Descripción	Tipo horas
Las actividades propuestas en el aula virtual deberán ser completadas en las fechas indicadas. No se receptarán trabajos, evaluaciones o actividades fuera del plazo indicado. La ética profesional será aplicada de tal manera que en todo trabajo o actividad escrita deberá agregarse la leyenda "por ética y por mi honor, declaro que este trabajo es fruto de mi propio esfuerzo". Los trabajos han de enviarse con el formato ApellidoNombre_Tarea#.pdf.	Autónomo
Las prácticas, evaluaciones y actividades realizadas en clase no son recuperables. La ética es contemplada todo momento, de tal manera, copias o intentos de copia serán calificados con 0 puntos. El uso de ChatGPT es aprobado, siempre y cuando no se lo utilice para opiniones personales, y que sea complementada con literatura y fuentes adicionales. No podrá ser utilizada en la redacción del examen final, el cual consiste en un capítulo de libro, pero si como elemento de consulta.	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

Autor	Título	Url
Cisco	Introduction to Cybersecurity	
Cisco Networking Academy	Cisco Networking Academy: Learn Cybersecurity, Python & More	https://www.netacad.com/es
Cisco Network Academy	Introducción a Ciberseguridad	https://skillsforall.com/course/introduction-to-cybersecurity?courseLang=es-XL
Cisco Network Academy	Ethical Hacking	https://skillsforall.com/course/ethical-hacker?courseLang=en-US

Software

Autor	Título	Url	Versión
Kali	Kali Linux		
Autopsy - Sleuthkit	Autopsy		4

Revista

Docente

Director/Junta

Fecha aprobación: 10/02/2024

Estado: Aprobado