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: ICC603
Paralelo: A
Periodo : Febrero-2025 a Junio-2025
Profesor: CRESPO MARTINEZ PAUL ESTEBAN
Correo electrónico: ecrespo@uazuay.edu.ec

Nivel: 6

Distribución de horas.

Docencia	Práctico	Autónomo:128		Total horas
		Sistemas de tutorías	Autónomo	
64	0	16	112	192

Prerrequisitos:

Código: ICC404 Materia: SISTEMAS OPERATIVOS II

2. Descripción y objetivos de la materia

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 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 se da a conocer por medio de la transferencia de conocimiento magistral, combinado con práctica 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.

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
bb1. 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.	
-Aprende a utilizar herramientas para la evaluación de vulnerabilidades en infraestructuras y sistemas de información	-Evaluación oral -Foros, debates, chats y otros -Proyectos -Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros
-Comprende el entorno de la ciberseguridad y sus implicaciones	-Evaluación oral -Foros, debates, chats y otros -Proyectos -Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros
-Conoce el proceso que se utiliza para acometer y defender una infraestructura de información	-Evaluación oral -Foros, debates, chats y otros -Proyectos -Prácticas de laboratorio -Reactivos -Resolución de ejercicios,

Resultado de aprendizaje de la carrera relacionados con la materia

Resultado de aprendizaje de la materia

Evidencias

casos y otros

Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Resolución de ejercicios, casos y otros	Trabajo sobre identificación de los activos de información y cálculo de riesgo	Principios básicos de la seguridad informática	APORTE	4	Semana: 2 (24/02/2025 al 01/03/2025)
Foros, debates, chats y otros	Investigación: Tendencias en la ciberseguridad en la sociedad y las empresas	Principios básicos de la seguridad informática	APORTE	2	Semana: 3 (05/03/2025 al 08/03/2025)
Reactivos	Prueba sobre fundamentos de ciberseguridad	Principios básicos de la seguridad informática, Sistema de Gestión de Seguridad de la Información	APORTE	4	Semana: 4 (10/03/2025 al 15/03/2025)
Prácticas de laboratorio	informe de prácticas de laboratorio sobre reconocimiento y escaneo	Ataque Informático, Técnicas de Hackeo	APORTE	5	Semana: 6 (24/03/2025 al 29/03/2025)
Prácticas de laboratorio	Informe de prácticas de laboratorio sobre ataques	Técnicas de Hackeo	APORTE	5	Semana: 8 (07/04/2025 al 12/04/2025)
Prácticas de laboratorio	Informe de práctica de laboratorio de evaluación forense. Debe presentarse en formato IEEE	Análisis forense	APORTE	5	Semana: 10 (21/04/2025 al 23/04/2025)
Prácticas de laboratorio	informe de prácticas sobre técnicas de ataque	Análisis forense, Respuesta a incidentes de seguridad y planes para la continuidad del negocio, Técnicas de Hackeo	APORTE	5	Semana: 11 (28/04/2025 al 03/05/2025)
Proyectos	Capítulo de libro sobre técnicas de ataque y contramedidas de seguridad. Guía de aseguramiento. Se realizará el texto y una presentación. Tarea en parejas.	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 (08-06-2025 al 21-06-2025)
Evaluación oral	Examen supletorio basado en preguntas de conocimiento y aplicación de la ciberseguridad en los procesos de TI	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
Vacca, J. R.	Morgan Kaufmann Publishers.	Computer and information security handbook	2019	
Bishop, M.	Addison-Wesley Professional.	Computer security: Art and science.	2018	
Bosworth, S.; Kabay, M. E.; Whyne, E.	CRC Press	Computer security basics	2011	
Whitman, M. E., Mattord, H. J.	Cengage Learning	Principles of Information Security	2019	
Stanger, S.; Medina, A.	O'Reilly Media	Cybersecurity for beginners	2019	
Crespo-Martínez Esteban		ECU@Risk: Una metodología para la gestión de riesgo	2017	
ISO	ISO	ISO/IEC 31000	2009	NO INDICA

Web

Software

Revista

Bibliografía de apoyo

Libros

Web

Software

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

Revista

Docente

Director/Junta

Fecha aprobación: 30/01/2025

Estado: Aprobado