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-2021 a Julio-2021
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.

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
5.1	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
6.1	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 -Prácticas de laboratorio -Trabajos prácticos - productos
-Investiga, conoce, analiza y determina los mecanismos de ataque y respuesta a incidentes informático	-Evaluación escrita -Prácticas de laboratorio -Trabajos prácticos - productos

Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Trabajos prácticos - productos	Aplicación de las normas ISO y metodologías de gestión de incidentes de seguridad	Principios básicos de la seguridad informática, Sistema de Gestión de Seguridad de la Información	APORTE DESEMPEÑO	3	Semana: 4 (05-ABR-21 al 10-ABR-21)
Prácticas de laboratorio	Informe de las prácticas de laboratorio en formato artículo	Análisis forense, Ataque Informático, Respuesta a incidentes de seguridad y planes para la continuidad del negocio, Técnicas de Hackeo	APORTE DESEMPEÑO	4	Semana: 8 (03-MAY-21 al 08-MAY-21)
Evaluación escrita	Evaluación en 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	APORTE DESEMPEÑO	3	Semana: 12 (31-MAY-21 al 05-JUN-21)
	APORTE CUMPLIMIENTO		APORTE CUMPLIMIENTO	10	Semana: 15 (21-JUN-21 al 26-JUN-21)
	APORTE ASISTENCIA		APORTE ASISTENCIA	10	Semana: 15 (21-JUN-21 al 26-JUN-21)
Trabajos prácticos - productos	Artículo: Tendencias de la ciberseguridad	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 FINAL ASINCRÓNICO	10	Semana: 17-18 (05-07-2021 al 18-07-2021)
Evaluación escrita	Examen teórico - práctico	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 FINAL SINCRÓNICO	10	Semana: 19 (19-JUL-21 al 24-JUL-21)
Trabajos prácticos - productos	Artículo: Tendencias de la ciberseguridad	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 ASINCRÓNICO	10	Semana: 17-18 (05-07-2021 al 18-07-2021)
Evaluación escrita	Examen teórico - práctico	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 SINCRÓNICO	10	Semana: 19 (19-JUL-21 al 24-JUL-21)

Metodología

Descripción	Tipo horas
El trabajo autónomo forma parte del componente de aporte al cumplimiento. Para ello, se evaluará la realización de las actividades propuestas en el campus, tales como controles de lectura, foros de discusión, revisión a casos empresariales, evaluaciones de aprendizaje, entre otros.	Autónomo
Las clases serán llevadas a cabo mediante zoom, aplicando herramientas virtuales que complementen el aprendizaje de los estudiantes.	Total docencia

Criterios de evaluación

Descripción	Tipo horas
Las tareas autónomas deberán ser entregadas en el plazo establecido. No se receptarán tareas fuera del plazo. Todas las tareas serán entregadas en el campus virtual. Los trabajos serán revisados mediante la plataforma Urkund a fin de validar citas bibliográficas no contempladas. Los estudiantes deberán realizar las tareas especificadas en el campus virtual para fortalecer el aprendizaje.	Autónomo
Para el Aporte a la asistencia: - Los estudiantes deberán ingresar a la sesión hasta máximo 10 minutos luego de la hora establecida para el inicio de clase. Además, deberán mantener encendidas las cámaras de video durante todo el tiempo que dure la sesión síncrona. La calificación será considerada en base al reglamento de la Facultad. Para el aporte al cumplimiento: - Se aplicará lo establecido en el reglamento de la Facultad. - Se considerará el cumplimiento de las actividades previstas en el campus virtual. No se receptarán actividades o tareas extratemporáneas. Para el aporte al desempeño: Para la calificación de los trabajos se tomará mucho en cuenta los siguientes factores: • Los trabajos copiados textualmente de Internet u otras fuentes sin haberlas citado serán consideradas como plagio y serán calificadas automáticamente con cero puntos. • Los documentos deben ser coherentes y mantener una adecuada redacción, ortografía y citas bibliográficas. • Las presentaciones con diapositivas son simplemente una guía de apoyo al expositor. Deben ser claras y no estar llenas de texto (se sugiere 7 líneas de texto como máximo). • En todas las pruebas y lecciones escritas se calificará procedimiento de resolución y resultados obtenidos, considerando coherencia y certeza en la aplicación de razonamientos y teorías. Además de la resolución de casos y ejercicios, todas las evaluaciones incluirán preguntas de razonamiento e interpretación de información. Las prácticas de laboratorio serán plasmadas en documentos en formato artículo científico, ya sea en IEEE o Springer (Las pautas serán dadas en clase). El trabajo final consiste en un artículo, cuyo eje temático es: "Tendencias de la ciberseguridad". Los mejores trabajos podrán ser seleccionados para presentación en congresos o revistas.	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

Autor	Editorial	Título	Año	ISBN
CANO, JEIMY	Alfaomega	COMPUTACIÓN FORENSE: DESCUBRIENDO LOS RASTROS INFORMÁTICOS	2011	NO INDICA

Web

Software

Autor	Título	Url	Versión
Kali	Kali Linux		

Revista

Docente

Director/Junta

Fecha aprobación: 08/03/2021

Estado: Aprobado