Ciberseguridad

INFORMACIÓN BÁSICA	
Código y Nombre	750024C – Ciberseguridad
Créditos	3
Horas de trabajo	Presenciales:3 horas Trabajo independiente: 6 horas
Unidad(es) Académica(s)	Escuela de Ingeniería de Sistemas y Computación Facultad de Ingeniería
Programas Académicos	Tecnología en desarrollo de software Ingeniería de Sistemas
Prerrequisitos	750010C - Fundamentos de redes 750016C - Simulación y Computación numérica
Validable	Sí
Habilitable	No
Tipo de Asignatura	Asignatura Profesional (AP)
La asignatura favorece la Formación General	
Si / **No**	**X**

DESCRIPCIÓN GENERAL DEL CURSO

Las amenazas de seguridad informática son cada vez más frecuentes, los sistemas computacionales y las redes de comunicaciones son cada vez más vulnerables a una diversidad de ataques físicos y lógicos porque cada vez son más complejas e integradas y los delincuentes tienen acceso desde cualquier lugar del mundo aprovechando las vulnerabilidades para robar información y dinero. Por esta razón existe una necesidad de especialistas en ciberseguridad, expertos forenses, expertos en seguridad de la información y Hackers éticos.

Esta es una asignatura interdisciplinaria, que incluye aspectos técnicos, legales, factores humanos, éticos y gestión del riesgo que tiene como objetivo introducir al estudiante en una disciplina basada en la informática que involucra tecnología, personas, información y procesos para permitir operaciones seguras en ambientes interconectados. El estudiante estará en capacidad de identificar los aspectos necesarios para que los sistemas, software y redes de comunicación sean seguros.

El curso permitirá desarrollar proyectos de ingeniería utilizando herramientas tecnológicas, en ambientes simulados, para contribuir en la reducción de vulnerabilidades en redes, sistemas y software con el fin de garantizar el monitoreo de infraestructura crítica.

No de Versión:	**	**No. y fecha acta unidad académica donde se aprobó:**	*(En caso de modificación en la sección "desarrollo del curso" debe actualizarse de lo contrario se mantiene)*
Fecha actualización:	**		

Competencias específicas	Resultados de Aprendizaje (RA)	%	Indicador de Logro (IL)	Indicador de logro / evidencia de aprendizaje	Contenidos
	R.A.1: Identifica las dimensiones de la ciberseguridad, entendiendo los componentes técnicos, regulatorios y de recursos humano necesarios , para que una red, un sistema o un software sea seguro	50	IL 1.1	Describe los principios de la ciberseguridad comprendiendo la función que cumple cada uno para el aseguramiento de las redes, sistemas y software seguros.	Introducción a la ciberseguridad
			IL 1.2	Describe el estado de los datos comprendiendo la necesidad de salvaguardar la información en cualquiera de ellos para el aseguramiento de las redes, sistemas y software seguros.	Las tres dimensiones de la ciberseguridad
			IL 1.3	Describe las estrategias tecnológicas, regulatorias y del recurso humano comprendiendo la necesidad de diseñar programas en cada una para el aseguramiento de las redes, sistemas y software seguros.	Tipos de Amenazas, vulnerabilidades y ataques a la ciberseguridad
	R.A.2: Aplica herramientas tecnológicas, en ambientes simulados, para contribuir en la reducción de vulnerabilidades en redes, sistemas y software	30	IL 2.1	Programa dispositivos inalámbricos comprendiendo el funcionamiento de los protocolos WEP/WPA2 PSK/WPA2 RADIUS para contribuir en la reducción de vulnerabilidades en las redes inalámbricas	Infraestructura segura - Seguridad de dispositivos de red y de capa de acceso
			IL 2.2	Emplea técnicas de control de acceso comprendiendo la lógica secuencial para la implementación de controles en acceso a los dispositivos y redes	Estrategias de mitigación de ataques
			IL 2.3	Configura dispositivos de red utilizando herramientas como NTP, SSH, SYSLOG, OSPF CON AUTENTICACION MD5 para implementar funcionalidades de seguridad en las redes de comunicación	Sistemas AAA Autenticación, autorización y auditoria
	R.A.3: Identifica componentes tecnológicos conociendo alternativas de mercado, para garantizar el monitoreo de infraestructura critica	20	IL 3.1	Describe las características de un sistema de observación comprendiendo la necesidad de la gestión y monitoreo para dar respuesta ante incidentes de seguridad en redes, sistemas y software	Monitoreo de infraestructura crítica

METODOLOGÍA

El curso se desarrolla en una clase semanal de tres horas. En esta asignatura se desarrollar actividades teóricos y prácticas usando herramientas de simulación.

RECURSOS DE APOYO

Para el desarrollo efectivo del curso se requiere de un salón con acceso a internet, con puestos individuales de trabajo, y que esté provista de video beam además de herramientas de docencia asistidas por tecnología disponibles en la institución, además de software de simulación como cisco packet tracer, eNSP, GNS3, Fortinet o Huawei

EVALUACIÓN DEL CURSO

La evaluación del curso incluye actividades de investigación, desarrollo de laboratorios y una exposición

Resultado de aprendizaje	Actividades evaluativas	Porcentaje parcial	Porcentaje total
R.A.1	Taller de investigación y Exposiciones		40
R.A.2	Laboratorios		40
R.A.3	Talleres		20

BIBLIOGRAFÍA

- Padilla Téllez, F. (2014). Ciberseguridad en infraestructuras críticas (Bachelor's thesis, Universidad Piloto de Colombia).
- Cano M, J. J. (2023, January). Security Risk Management and Cybersecurity: From the Victim or from the Adversary?. In Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022 (pp. 1-8). Cham: Springer International Publishing.
- Curso de Cybersecurity Essentials Español Cisco Networking Academy