Programa de asignatura
por competencias de educación superior

Sección I. Identificación del Curso

Tabla 1. Identificación de la Planificación del Curso.

Actualización:	Septiembre 26, 2022				
Carrera:	Ingeniería en Desarrollo de Software		**Asignatura:**	Hacking ético	
Academia:	Desarrollo de software /		**Clave:**	19SDSSI01	
Módulo formativo:	Internet de las cosas		**Seriación:**	- -	
Tipo de curso:	Presencial		**Prerrequisito:**	- -	
Semestre:	Sexto	**Créditos:** 6.75	**Horas semestre:**	108 horas	
Teoría:	2 horas	**Práctica:** 2 horas	**Trabajo indpt.:**	2 horas	**Total x semana:** 6 horas

Sección II. Objetivos educacionales

Tabla 2. Objetivos educacionales

Objetivos educacionales		Criterios de desempeño	Indicadores
1	Los egresados gestionarán recursos relacionados con el desarrollo de software en alguna organización.	Los egresados podrán aplicar metodologías en el desarrollo de proyectos en el contexto laboral.	20% de los egresados aplicarán metodologías en el desarrollo de software en su contexto laboral.
2	Los egresados diseñarán e implementarán soluciones innovadoras mediante el uso de tecnologías de la información.	Los egresados participarán activamente en el ciclo de desarrollo e integración continuos	25% de los egresados desempeñarán labores de desarrollo e integración continuos.
3	Los egresados desarrollarán conocimiento especializado que les permite enfocarse en un área del conocimiento específico del desarrollo de software.	Los egresados desempeñarán actividades orientadas al aseguramiento de los activos de información de manera resiliente, la gestión de la infraestructura de redes y comunicaciones, o integrando hardware y software para crear soluciones IoT; así como el uso de inteligencia artificial para gestionar datos y reconocer patrones que determinen oportunidades de negocio en las organizaciones.	5% de los egresados desempeñarán labores en desarrollo de soluciones IoT.
4	Los egresados serán capaces de emprender un negocio basado en el desarrollo de un producto o servicio de tecnologías de la información, aportando valor a la generación de empleos e incrementar el bienestar económico y social, de forma ecológica y sustentable.	Los egresados serán capaces de emprender un negocio basado en el desarrollo propio de un producto o servicio de tecnologías de la información.	2% de los egresados tendrán participación en el acta constitutiva de una empresa creada a partir del desarrollo de software para ofrecer un producto o servicio.

Atributos de egreso de plan de estudios		Criterios de desempeño	Componentes
1	Aplicar y analizar procesos de diseño de ingeniería para generar una experiencia de usuario que asegure cubrir las necesidades como las expectativas de clientes y partes interesadas, utilizando y gestionando la infraestructura de red necesaria.	- Aplicar metodologías en el desarrollo de proyectos en el contexto laboral. - Dirigir proyectos en los que tiene personal a su cargo.	1.1 Conceptos relacionados con vulnerabilidad y amenazas. 1.2 Escenarios y tipos de ataques. 1.5 Definición de evaluación de seguridad, hacking ético y pruebas de penetración. 1.6 Tipos de pruebas de penetración. 1.7 Metodologías. 1.8 Planeación de la revisión. 1.9 Ingeniería social.
2	Identificar su responsabilidad ética y profesional con el entorno sociocultural y ambiental para aplicar estándares, así como fundamentos legales y normativos, aportando valor al contexto social y sustentable.	- Desempeñar actividades orientadas al aseguramiento de los activos de información de manera resiliente.	4.1 Bastion Host. 4.2 Componentes serverless. 4.3 Manejador de secretos. 4.4 Seguridad de la cuenta en la nube.
3	Reconocer la mejora continua como parte de su desarrollo profesional para mantener un perfil actualizado en desarrollo de software para el diseño e implementación de productos y servicios basados en tecnologías con las tendencias emergentes.	- Desempeñar actividades orientadas al aseguramiento de los activos de información de manera resiliente para gestionar datos y reconocer patrones que determinen oportunidades de negocio en las organizaciones.	1.7 Metodologías. 1.10 Foros, blogs y redes sociales. 1.11 APT. 1.12 Legislación. 3.2 Identificación de servicios y Fingerprinting. 4.5 Logs y trazabilidad de la cuenta. 4.6 Logs y trazabilidad de los componentes.

Sección III. Atributos de la asignatura

Tabla 3. Atributos de la asignatura

<table>
<tr><th colspan="3">Problema a resolver</th></tr>
<tr><td colspan="3">Analizar la seguridad de los sistemas informáticos corporativos emulando lo que podría ocurrir en el peor de los escenarios para identificar vulnerabilidades existentes, me?todos y te?cnicas de aprovechamiento, a fin de establecer procedimientos de mitigación para salvaguardar los activos de la organización.</td></tr>
<tr><th colspan="3">Atributos (competencia específica) de la asignatura</th></tr>
<tr><td colspan="3">Diseñar e implementar diversas estrategias y procesos para identificar brechas de seguridad en los sistemas de software corporativos.</td></tr>
<tr><th colspan="2">Aportación a la competencia específica</th><th>Aportación a las competencias transversales</th></tr>
<tr><td>Saber</td><td>Saber hacer</td><td>Saber Ser</td></tr>
<tr><td>- Identificar las características de la organización objetivo.
- Enlistar las herramientas de reconocimiento.
- Identificar las metodologías utilizadas en ingeniería social.
- Enlistar las técnicas y herramientas para el escaneo de puertos.
- Identificar las técnicas y herramientas de detección de vulnerabilidades.</td><td>- Desarrollar un reporte técnico para el establecimiento de un vector de ataque.
- Seleccionar las herramientas de detección de reconocimientoy vulnerabilidades.
- Implementar las herramientas de detección de vulnerabilidades.
- Evaluar las metodologías existentes para ingeniería social.</td><td>- Realizar procesos adecuados de diseño de ingeniería, reconociendo sus responsabilidades éticas y profesionales.
- Entrega en tiempo y forma de sus actividades.
- Sus trabajos son de autoría propia.</td></tr>
<tr><th colspan="3">Producto integrador de la asignatura, considerando los avances por unidad</th></tr>
<tr><td colspan="3">Diseño e implementación de una prueba de penetración para determinar el alcance de los fallos de seguridad de un sistema.</td></tr>
</table>

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.1. Desglose específico de la unidad "Hacking ético y pruebas de penetración."

Número y nombre de la unidad:	1. Hacking ético y pruebas de penetración.					
Tiempo y porcentaje para esta unidad:	Teoría:	10 horas	Práctica:	10 horas	Porcentaje del programa:	27.78%
Aprendizajes esperados:	Conocer e identificar recursos de hackeo seguros y fuentes seguras de informacio?n, sin riesgo de estar quedando expuestos.					

Temas y subtemas (secuencia)	**Criterios de desempeño**	**Estrategias didácticas**	**Estrategias de evaluación**	**Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)**
1.1 Conceptos relacionados con vulnerabilidad y amenazas. 1.2 Escenarios y tipos de ataques. 1.3 Conceptos de encriptación. 1.5 Definición de evaluación de seguridad, hacking ético y pruebas de penetración. 1.6 Tipos de pruebas de penetración. 1.7 Metodologías. 1.8 Planeación de la revisión. 1.9 Ingeniería social. 1.10 Foros, blogs y redes sociales. 1.11 APT. 1.12 Legislación.	Saber: - Conocer y analizar la terminología básica del hacking ético con el objetivo de adentrarse en el área. - Conocer las habilidades que debe poseer un hacker para proporcionar seguridad en la empresa. - Conocer los diferentes tipos de Malware y técnicas de ataque más comunes. Saber hacer: - Identificar recursos de hackeo seguros y fuentes seguras de información, sin riesgo de estar quedando expuestos.	- Preguntas intercaladas. - Presentación de material teórico a través de diversos medios (diapositivas, proyector, videoconferencia, computadora, internet). - Tareas de investigación.	Evaluación diagnóstica: - Rescatar conocimiento previo. Evaluación formativa: - Mapa mental, mapa conceptual, resumen. - Actividades, ejercicios, prácticas. Evaluación sumativa: - Examen.	Análisis de vulnerabilidades de sitios web y sistemas operativos.

Continuación: Tabla 4.1. Desglose específico de la unidad "Hacking ético y pruebas de penetración."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	Ser: - Realizar procesos adecuados de diseño de ingeniería, reconociendo sus responsabilidades éticas y profesionales. - Entrega en tiempo y forma de sus actividades. - Sus trabajos son de autoría propia.			

Bibliografía

- Astudillo, B. K. (2019). Hacking ético. 3a. ed. Colombia: Ediciones de la U.
- Ortega, J.M. (2018). Hacking ético con herramientas Python. España: RA-MA Editorial.
- Roa, J.F. (2013). Seguridad informática. España: McGraw-Hill.
- Lewis, E. (2020). Ciberseguridad: Guía completa para principiantes, aprende todo de la ciberseguridad de la Aa la Z. Independently Published.
- Harper, A.; Harris, S.; Ness, J.; Eagle, C., Gray, C. (2011). Hat Hacking The Ethical Hackers Handbook. 3rd Edition. USA: McGraw-Hill/Osborne Media
- Simpson, M.; Backman, K.; Corley, J. (2011). Hands-On Ethical Hacking and Network Defense. USA: Course Technology.
- Accissi, M. (2011). Seguridad Informa?tica. Ethical Hacking. Barcelona: ENI.

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.2. Desglose específico de la unidad "Creación y manejo de laboratorio para la ejecución de penetración."

Número y nombre de la unidad:	2. Creación y manejo de laboratorio para la ejecución de penetración.					
Tiempo y porcentaje para esta unidad:	Teoría:	10 horas	Práctica:	10 horas	Porcentaje del programa:	27.78%
Aprendizajes esperados:	Conocer e implementar el entorno de pruebas para implementar los vectores de ataque.					

Temas y subtemas (secuencia)	**Criterios de desempeño**	**Estrategias didácticas**	**Estrategias de evaluación**	**Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)**
2.1 Fases de un pentest. 2.2 La autorización. 2.3 Linux. 2.3.1 El framework Metasploit. 2.3.1 Instalación y personalización. 2.4 Windows. 2.4.1 Herramientas a utilizar.	Saber: - Conocer el proceso de diseño de una prueba de penetración y prueba. - Conocer el sistema operativo Linux. Saber hacer: - Implementar el entorno de pruebas para implementar los vectores de ataque. - Instalar, configurar y puesta a punto de un sistema Linux. Ser: - Realizar procesos adecuados de diseño de ingeniería, reconociendo sus responsabilidades éticas y profesionales.	- Presentación de material teórico a través de diversos medios (Diapositivas, proyector, videoconferencia, computadora, internet). - Tareas de investigación. - Prácticas.	Evaluación formativa: - Mapa mental, mapa conceptual, resumen. - Actividades, ejercicios, prácticas. Evaluación sumativa: - Examen.	- Reporte de prácticas sobre los vectores de ataque.

Continuación: Tabla 4.2. Desglose específico de la unidad "Creación y manejo de laboratorio para la ejecución de penetración."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	- Entrega en tiempo y forma de sus actividades. - Sus trabajos son de autoría propia.			

Bibliografía

- Astudillo, B. K. (2019). Hacking ético. 3a. ed. Colombia: Ediciones de la U.
- Ortega, J.M. (2018). Hacking ético con herramientas Python. España: RA-MA Editorial.
- Roa, J.F. (2013). Seguridad informática. España: McGraw-Hill.
- Lewis, E. (2020). Ciberseguridad: Guía completa para principiantes, aprende todo de la ciberseguridad de la Aa la Z. Independently Published.
- Harper, A.; Harris, S.; Ness, J.; Eagle, C., Gray, C. (2011). Hat Hacking The Ethical Hackers Handbook. 3rd Edition. USA: McGraw-Hill/Osborne Media
- Simpson, M.; Backman, K.; Corley, J. (2011). Hands-On Ethical Hacking and Network Defense. USA: Course Technology.
- Accissi, M. (2011). Seguridad Informa?tica. Ethical Hacking. Barcelona: ENI.

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.3. Desglose específico de la unidad "Fases de las pruebas de penetración a infraestructura tecnológica."

Número y nombre de la unidad:	3. Fases de las pruebas de penetración a infraestructura tecnológica.					
Tiempo y porcentaje para esta unidad:	Teoría:	8 horas	Práctica:	8 horas	Porcentaje del programa:	22.22%
Aprendizajes esperados:	Conocer y usar las herramientas de escaneo de puertos para obtener información de vulnerabilidades de un sistema.					

Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)
3.1 Escaneo de puertos. 3.2 Identificación de servicios y Fingerprinting. 3.3 Análisis remoto de vulnerabilidades. 3.4 Ocultando orígenes (anonimizadores, proxies anónimos, TOR).	Saber: - Conocer las herramientas para realizar un análisis remoto de vulnerabilidades. - Conocer las herramientas para anonimizar. Saber hacer: - Utilizar herramientas de escaneo de puertos para obtener información de vulnerabilidades de un sistema. - Identificar un objetivo y hacer reconocimiento utilizando internet WHOIS, DNS, WebSite y Google Hacking. Ser: - Realizar procesos adecuados de diseño de ingeniería, reconociendo sus	- Presentación de material teórico a través de diversos medios (Diapositivas, proyector, videoconferencia, computadora, internet). - Tareas de investigación. - Prácticas.	Evaluación formativa: - Mapa mental, mapa conceptual, resumen. - Actividades, ejercicios, prácticas. Evaluación sumativa: - Examen.	- Reporte de prácticas sobre los análisis remotos de vulnerabilidades.

Continuación: Tabla 4.3. Desglose específico de la unidad "Fases de las pruebas de penetración a infraestructura tecnológica."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	responsabilidades éticas y profesionales. - Entrega en tiempo y forma de sus actividades. - Sus trabajos son de autoría propia.			

Bibliografía

- Astudillo, B. K. (2019). Hacking ético. 3a. ed. Colombia: Ediciones de la U.
- Ortega, J.M. (2018). Hacking ético con herramientas Python. España: RA-MA Editorial.
- Roa, J.F. (2013). Seguridad informática. España: McGraw-Hill.
- Lewis, E. (2020). Ciberseguridad: Guía completa para principiantes, aprende todo de la ciberseguridad de la Aa la Z. Independently Published.
- Harper, A.; Harris, S.; Ness, J.; Eagle, C., Gray, C. (2011). Hat Hacking The Ethical Hackers Handbook. 3rd Edition. USA: McGraw-Hill/Osborne Media
- Simpson, M.; Backman, K.; Corley, J. (2011). Hands-On Ethical Hacking and Network Defense. USA: Course Technology.
- Accissi, M. (2011). Seguridad Informa?tica. Ethical Hacking. Barcelona: ENI.

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.4. Desglose específico de la unidad "Seguridad en la nube."

Número y nombre de la unidad:	4. Seguridad en la nube.					
Tiempo y porcentaje para esta unidad:	Teoría:	8 horas	Práctica:	8 horas	Porcentaje del programa:	22.22%
Aprendizajes esperados:	Conocer los controles, normas, tecnologías y procedimientos que se utilizan para proteger los datos en la nube.					

Temas y subtemas (secuencia)	**Criterios de desempeño**	**Estrategias didácticas**	**Estrategias de evaluación**	**Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)**
4.1 Bastion Host. 4.2 Componentes serverless. 4.3 Manejador de secretos. 4.4 Seguridad de la cuenta en la nube. 4.5 Logs y trazabilidad de la cuenta. 4.6 Logs y trazabilidad de los componentes.	Saber: - Conocer los controles, normas, tecnologías y procedimientos que se utilizan paraproteger los datos y las aplicaciones. Saber hacer: - Implementar mecanismos para proteger la integridad de las aplicaciones, los datos y la infraestructura virtual basados en la nube. Ser: - Realizar procesos adecuados de diseño de ingeniería, reconociendo sus responsabilidades éticas y profesionales.	- Presentación de material teórico a través de diversos medios (Diapositivas, proyector, videoconferencia, computadora, internet). - Tareas de investigación. - Prácticas.	Evaluación formativa: - Mapa mental, mapa conceptual, resumen. - Actividades, ejercicios, prácticas. Evaluación sumativa: - Examen.	- Reporte de prácticas sobre las vulnerabilidades en la nube.

Continuación: Tabla 4.4. Desglose específico de la unidad "Seguridad en la nube."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	- Entrega en tiempo y forma de sus actividades. - Sus trabajos son de autoría propia.			

Bibliografía

- Astudillo, B. K. (2019). Hacking ético. 3a. ed. Colombia: Ediciones de la U.
- Ortega, J.M. (2018). Hacking ético con herramientas Python. España: RA-MA Editorial.
- Roa, J.F. (2013). Seguridad informática. España: McGraw-Hill.
- Lewis, E. (2020). Ciberseguridad: Guía completa para principiantes, aprende todo de la ciberseguridad de la Aa la Z. Independently Published.
- Harper, A.; Harris, S.; Ness, J.; Eagle, C., Gray, C. (2011). Hat Hacking The Ethical Hackers Handbook. 3rd Edition. USA: McGraw-Hill/Osborne Media
- Simpson, M.; Backman, K.; Corley, J. (2011). Hands-On Ethical Hacking and Network Defense. USA: Course Technology.
- Accissi, M. (2011). Seguridad Informa?tica. Ethical Hacking. Barcelona: ENI.

V. Perfil docente

Tabla 5. Descripción del perfil docente

Perfil deseable docente para impartir la asignatura
Carrera(s): - Ingeniería en Sistemas, titulado o carrera afín. o carrera afín - Manejo de TIC´s. Con habilidades pedagógicas y uso de metodologías alternativas de enseñanza. - Experiencia mínima de dos años - Ingeniero titulado o superior