PROGRAMA EDUCATIVO:

LICENCIATURA EN INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN E INNOVACIÓN DIGITAL
EN COMPETENCIAS PROFESIONALES

PROGRAMA DE ASIGNATURA: SEGURIDAD INFORMÁTICA

CLAVE: E-SEIN-3

Propósito de aprendizaje de la Asignatura	El estudiante desarrollará un plan maestro de seguridad de sistemas mediante metodologías y herramientas de seguridad para asegurar la integridad, confidencialidad y disponibilidad de la información en entornos organizacionales.
Competencia a la que contribuye la asignatura	Desarrollar soluciones innovadoras de integración de tecnologías de la información mediante metodologías y herramientas de seguridad informática, internet de las cosas, sistemas inteligentes y administración de proyectos; con base en las normas y estándares aplicables para atender las áreas de oportunidad, resolver las necesidades y optimizar los procesos y recursos de diversos sectores.

Tipo de competencia	Cuatrimestre	Créditos	Modalidad	Horas por semana	Horas Totales
Específica	**7**	**5.63**	**Escolarizada**	**6**	**90**

Unidades de Aprendizaje	Horas del Saber	Horas del Saber Hacer	Horas Totales
I. Introducción a la ciberseguridad y dispositivos finales	12	18	30
II. Gestión de amenazas cibernéticas	7	11	18
III. Hacking ético y vulnerabilidades	12	18	30
IV. Herramientas de análisis y reporteo	5	7	12
Totales	**36**	**54**	**90**

Funciones	Capacidades	Criterios de Desempeño
Implementar un plan maestro de seguridad de sistemas, datos e infraestructura, mediante la evaluación de vulnerabilidad, pruebas de penetración y fortalecimiento de la seguridad para garantizar su protección.	Planificar un documento maestro de seguridad de sistemas, datos e infraestructura mediante la identificación y organización de requisitos de seguridad y la aplicación de defensa profunda.	Elaborar un plan maestro de seguridad de sistemas, datos e infraestructura que contenga lo siguiente: - Diagnóstico que identifique los requisitos de seguridad. - Análisis de riesgos. - Tabla de integración de estrategias, iniciativas y proyectos orientados a la mejora de la seguridad, con descripción detallada, justificación y presupuesto de recursos materiales y humanos para cada una de las siete capas: 1) Políticas y procedimientos recomendados. 2) Seguridad física. 3) Perímetro 4) Red interna 5) Host 6) Aplicación 7) Datos - Resultados de la valoración inicial de la organización - Análisis detallado de capacidades requeridas por el personal

		- Cronograma de implementación. - Conclusiones.
	Implementar un plan maestro de seguridad de sistemas, datos e infraestructura mediante la creación de políticas, seguridad física, perímetro de la red, procedimientos y controles para proteger la información.	Elaborar un informe técnico que documente la implementación del plan maestro de seguridad, que contenga lo siguiente: - Introducción - Justificación - Diagnóstico (detección de necesidades y análisis del contexto). - Contexto y análisis de riesgos. - Estructura organizacional de seguridad (roles, responsabilidades, etc.) - Controles de seguridad. - Listado y descripción de las políticas, procedimientos y controles - Bitácora y registro de la implementación de políticas, procedimientos y controles. - Costos de la inversión. - Conclusiones.
	Evaluar un plan maestro de seguridad de sistemas, datos e infraestructura mediante la determinación de la eficacia del sistema de gestión de seguridad, identificando áreas de oportunidad para aplicar mejoras a los procesos y controles del plan maestro de seguridad para proteger la información ante nuevas vulnerabilidades.	Informe técnico de la evaluación de la ejecución de un plan maestro de seguridad, que contenga lo siguiente: - Estrategias de monitoreo - Gestión de incidentes y respuesta a incidentes. - Evaluación de la efectividad y madurez de las estrategias implementadas por la organización en términos de seguridad. - Resultados de las pruebas tecnológicas simuladas aplicadas a las estrategias de seguridad de la organización en un ambiente controlado (pruebas de penetración y análisis de vulnerabilidades) - Cumplimiento y auditoría - Identificación de áreas de oportunidad - Plan de mejora continua - Conclusiones.

UNIDADES DE APRENDIZAJE

Unidad de Aprendizaje	I. Introducción a la ciberseguridad y dispositivos finales.					
Propósito esperado	El estudiante evaluará y asegurará la integridad de la información y los dispositivos finales, para proteger los datos y la privacidad de la organización frente a vulnerabilidades y ataques.					
Tiempo Asignado	**Horas del Saber**	12	**Horas del Saber Hacer**	18	**Horas Totales**	30

Temas	Saber Dimensión Conceptual	Saber Hacer Dimensión Actuacional	Ser y Convivir Dimensión Socioafectiva
Principios básicos de seguridad informática	Identificar los principios básicos de la ciberseguridad.	Establecer medidas de protección de datos. Gestionar asignación de responsabilidades de ciberseguridad. Evaluar debilidades y vulnerabilidades de los sistemas Configurar medidas de seguridad de la red. Establecer configuraciones y prácticas seguras en los sistemas operativos. Gestionar protección de los dispositivos finales.	Desarrollar el pensamiento analítico a través de la identificación de conceptos para resolver problemas en su formación académica o su entorno. Asumir la responsabilidad y honestidad para realizar actividades en forma individual y en equipo en forma proactiva. Ejercer liderazgo en la práctica de laboratorio, coordinando las actividades para el buen resultado de la práctica o proceso a desarrollar.
Protegiendo tus datos y privacidad, protegiendo la organización	Describir la aplicación de medidas de protección de datos. Describir los métodos avanzados de autenticación.		
Asignación de responsabilidades de la información (CIO+CISO)	Identificar los roles clave en la gestión de la ciberseguridad.		
Evaluación de vulnerabilidades por tecnología y por aplicación	Describir los fundamentos de los ataques Describir las posibles debilidades en los sistemas. Identificar las técnicas utilizadas por los atacantes.		
Asegurando un sistema informático	Identificar las medidas de seguridad de la infraestructura de red. Identificar las configuraciones y prácticas seguras en los sistemas operativos.		

	Describir la protección de los dispositivos utilizados por los usuarios finales.		

Proceso Enseñanza-Aprendizaje			
Métodos y técnicas de enseñanza	Medios y materiales didácticos	Espacio Formativo	
		Aula	
Prácticas en Laboratorio Análisis de Casos Simulación	Equipos y Hardware de red Software y Herramientas de Simulación. Documentación y Manuales Recursos de Aprendizaje en Línea Materiales de Referencia. Laboratorios y Espacios de Práctica Herramientas de virtualización y automatización.	**Laboratorio / Taller**	X

Proceso de Evaluación		
Resultado de Aprendizaje	Evidencia de Aprendizaje	Instrumentos de evaluación
Los estudiantes identifican los conceptos de seguridad informática, protección de datos y la gestión de responsabilidades en la organización, asegurando la red, sistemas operativos y dispositivos finales.	A partir de un portafolio de evidencias de prácticas de laboratorio los estudiantes deben proteger datos, asegurar sistemas operativos y dispositivos finales siguiendo protocolos de seguridad.	Proyectos grupales y/o individuales Rúbrica.

Unidad de Aprendizaje	II. Gestión de amenazas cibernéticas					
Propósito esperado	El estudiante gestionará amenazas cibernéticas y registrará eventos de vulnerabilidad, para fortalecer la seguridad y la resiliencia de los sistemas informáticos de la organización.					
Tiempo Asignado	**Horas del Saber**	7	**Horas del Saber Hacer**	11	**Horas Totales**	18

Temas	Saber Dimensión Conceptual	Saber Hacer Dimensión Actuacional	Ser y Convivir Dimensión Socioafectiva
Capacidad de análisis de riesgos	Describir los conceptos de administración de redes. Explicar el funcionamiento de los protocolos CDP y LLDP. Describir el protocolo NTP y su importancia en las redes. Explicar el funcionamiento del protocolo SNMP. Describir la función de syslog en la administración de redes.	Identificar riesgos potenciales de un sistema informático.	Desarrollar el pensamiento analítico a través de la identificación de conceptos para resolver problemas en su formación académica o su entorno. Asumir la responsabilidad y honestidad para realizar actividades en forma individual y en equipo en forma proactiva. Ejercer liderazgo en la práctica de laboratorio, coordinando las actividades para el buen resultado de la
SIE (Security Information and Event Management)	Identificar las características de las redes jerárquicas y su importancia en la escalabilidad de redes.	Describir los sistemas de gestión de eventos de seguridad.	
Registro de eventos de vulnerabilidad	Identificar los dispositivos de hardware utilizados en redes y la importancia de su mantenimiento. Describir los procedimientos de mantenimiento de switches y routers.	Identificar la documentación de eventos de seguridad.	

Bitácora y registro de implementación de políticas, procedimientos y controles.	Explicar los principios del diseño de red.	Identificar los registros detallados de la implementación de políticas y procedimientos de seguridad.	práctica o proceso a desarrollar.

Proceso Enseñanza-Aprendizaje			
Métodos y técnicas de enseñanza	Medios y materiales didácticos	Espacio Formativo	
		Aula	
Prácticas en Laboratorio Análisis de Casos Simulación	Equipos y Hardware de red Software y Herramientas de Simulación. Documentación y Manuales Recursos de Aprendizaje en Línea Materiales de Referencia. Laboratorios y Espacios de Práctica Herramientas de virtualización y automatización.	**Laboratorio / Taller**	X

Proceso de Evaluación		
Resultado de Aprendizaje	Evidencia de Aprendizaje	Instrumentos de evaluación
Los estudiantes comprenden y analizan la gestión de amenazas cibernéticas, utilizando capacidades de análisis de riesgos, SIE (Security Information and Event Management), y registro de eventos de vulnerabilidad, implementando políticas, procedimientos y controles efectivos en la organización.	A partir de un caso práctico, los estudiantes deberán identificar y documentar amenazas, vulnerabilidades y posibles impactos en la organización, proponiendo estrategias de mitigación. La evidencia de aprendizaje incluirá la presentación de un informe técnico.	Proyectos grupales y/o individuales Rúbrica

Unidad de Aprendizaje	III. Hacking ético y vulnerabilidades					
Propósito esperado	El estudiante realizará pruebas de vulnerabilidad y penetración en sistemas informáticos, para identificar y mitigar riesgos de seguridad, garantizando la integridad y confidencialidad de la información.					
Tiempo Asignado	**Horas del Saber**	12	**Horas del Saber Hacer**	18	**Horas Totales**	30

Temas	Saber Dimensión Conceptual	Saber Hacer Dimensión Actuacional	Ser y Convivir Dimensión Socioafectiva
Fundamentos de Ethical Hacking y pentest	Identificar los conocimientos básicos y técnicas de hacking ético.	Administrar tecnologías de la información mediante el enfoque Gobernanza, riesgo y cumplimiento. Organizar controles detallados de los activos de TI. Evaluar la seguridad mediante simulaciones de ataques. Administrar la seguridad de diferentes tipos de redes.	Desarrollar el pensamiento analítico a través de la identificación de conceptos para resolver problemas en su formación académica o su entorno. Asumir la responsabilidad y honestidad para realizar actividades en forma individual y en equipo en forma proactiva. Ejercer liderazgo en la práctica de laboratorio, coordinando las actividades
Gobernanza, riesgo y cumplimiento.	Describir las normativas y gestión de riesgos. Relacionar las necesidades de la red con las medidas de seguridad.		
Manejo de inventarios.	Explicar el control detallado de los activos de TI.		
Pruebas de vulnerabilidad y de penetración (caja negra y caja blanca)	Identificar vulnerabilidades y puntos débiles en los sistemas. Describir el uso de simulaciones de ataques.		
Explotando vulnerabilidades en redes inalámbricas e inalámbricas.	Identificar los diferentes tipos de amenazas en redes wifi. Describir las vulnerabilidades en diferentes tipos de redes.		

OWASP	Describir las vulnerabilidades comunes en aplicaciones web.	Gestionar vulnerabilidades comunes en aplicaciones web. Mitigar diferentes tipos de vulnerabilidades.	para el buen resultado de la práctica o proceso a desarrollar.
Vulnerabilidades comunes	Identificar diferentes tipos de vulnerabilidades (basadas en inyección, autenticación, autorización, XSS, CSRF/XSRF, Clickjacking, falta de configuración, inclusión de archivos, prácticas inseguras de programación)		

Proceso Enseñanza-Aprendizaje			
Métodos y técnicas de enseñanza	Medios y materiales didácticos	Espacio Formativo	
		Aula	
Prácticas en Laboratorio Análisis de Casos Simulación	Equipos y Hardware de red Software y Herramientas de Simulación. Documentación y Manuales Recursos de Aprendizaje en Línea Materiales de Referencia. Laboratorios y Espacios de Práctica Herramientas de virtualización y automatización.	**Laboratorio / Taller**	X

Proceso de Evaluación		
Resultado de Aprendizaje	Evidencia de Aprendizaje	Instrumentos de evaluación
Los estudiantes comprenden y evalúan las técnicas de hacking ético y las vulnerabilidades en los sistemas, aplicando pruebas de penetración y técnicas de explotación de vulnerabilidades fortaleciendo la seguridad de las redes y sistemas de la organización.	A partir de un caso práctico, los estudiantes deberán ejecutar pruebas de penetración tipo caja negra y caja blanca en un entorno simulado, documentando los hallazgos y proponiendo soluciones a las vulnerabilidades encontradas. La evidencia de aprendizaje incluirá la presentación de un informe técnico.	Proyectos grupales y/o individuales Estudios de casos

Unidad de Aprendizaje	IV. Herramientas de análisis y reporteo					
Propósito esperado	El estudiante utilizará herramientas de monitoreo y análisis, para implementar estrategias de defensa y comunicación post ataque, asegurando la continuidad y seguridad de los sistemas informáticos.					
Tiempo Asignado	**Horas del Saber**	5	**Horas del Saber Hacer**	7	**Horas Totales**	12

Temas	Saber Dimensión Conceptual	Saber Hacer Dimensión Actuacional	Ser y Convivir Dimensión Socioafectiva
Monitoreo de sistemas	Describir los elementos necesarios para monitorear sistemas informáticos. Explicar los métodos para la vigilancia continua de los sistemas informáticos.	Establecer métodos de vigilancia continua de sistemas informáticos.	Desarrollar el pensamiento analítico a través de la identificación de conceptos para resolver problemas en su formación académica o su entorno. Asumir la responsabilidad y honestidad para realizar actividades en forma individual y en equipo en forma proactiva. Ejercer liderazgo en la práctica de laboratorio,
Estrategias post ataque	Describir las medidas reactivas y preventivas después de un incidente de seguridad. Describir una comunicación efectiva y registro detallado de todas las acciones correctivas.	Establecer medidas reactivas y preventivas después de un incidente de seguridad. Documentar detalladamente todas las acciones correctivas.	
Scripts de análisis y pentest.	Identificar los scripts para analizar y probar la seguridad de los sistemas. Describir situaciones prácticas y reales de seguridad de sistemas.	Proponer scripts de análisis y pruebas de seguridad de sistemas.	

			coordinando las actividades para el buen resultado de la práctica o proceso a desarrollar.

Proceso Enseñanza-Aprendizaje			
Métodos y técnicas de enseñanza	Medios y materiales didácticos	Espacio Formativo	
		Aula	
Prácticas en Laboratorio Análisis de Casos Equipos colaborativos.	Equipos y Hardware de red Software y Herramientas de Simulación. Documentación y Manuales Recursos de Aprendizaje en Línea Materiales de Referencia. Laboratorios y Espacios de Práctica Herramientas de virtualización y automatización.	**Laboratorio / Taller**	X

Proceso de Evaluación		
Resultado de Aprendizaje	Evidencia de Aprendizaje	Instrumentos de evaluación
Los estudiantes identifican la aplicación de herramientas de monitoreo y análisis, desarrollando estrategias de defensa post ataque y comunicación efectiva de acciones de remediación.	A partir de un portafolio de evidencias de prácticas los estudiantes deben desarrollar y ejecutar scripts de análisis, describir estrategias de comunicación y procedimientos de registro de acciones de remediación post ataque, incluyendo ejemplos prácticos y casos de estudio.	Proyectos grupales y/o individuales Estudios de casos

Perfil idóneo del docente		
Formación académica	**Formación Pedagógica**	**Experiencia Profesional**
Ingeniería en Sistemas Computacionales Ingeniería en Telecomunicaciones. Ingeniería en ciberseguridad.	Manejo de herramientas didácticas y de evaluación experiencia en técnicas de manejo de grupos conocimiento de educación basada en competencias	Experiencia laboral como analista de seguridad, consultor de seguridad, administrador de sistemas de seguridad, auditor de seguridad. Conocimiento práctico en el uso de herramientas de monitoreo y análisis de seguridad (SIEM, IDS/IPS, firewalls, etc.). Certificaciones CISSP, CEH, CISM, CompTIA Security+, OSCP. Cursos de actualización continua en ciberseguridad.

Referencias bibliográficas					
Autor	Año	Título del documento	Lugar de publicación	Editorial	ISBN
William Stallings, Lawrie Brown	2019	Computer Security: Principles and Practice	Boston, MA, USA	Pearson	978-0134794105
Michael E. Whitman, Herbert J. Mattord	2021	Principles of Information Security	Boston, MA, USA	Cengage Learning	978-0357506416
Dafydd Stuttard, Marcus Pinto	2020	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws	Indianapolis, IN, USA	Wiley	978-1118026472

William Stallings	2019	Network Security Essentials: Applications and Standards	Boston, MA, USA	Pearson	978-0134527338
Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short	2018	Cybersecurity Essentials	Indianapolis, IN, USA	Wiley	978-1119362395
David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni	2019	Metasploit: The Penetration Tester's Guide	San Francisco, CA, USA	No Starch Press	978-1593275648
Jon Erickson	2018	Hacking: The Art of Exploitation	San Francisco, CA, USA	No Starch Press	978-1593271442
David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask	2018	Security Information and Event Management (SIEM) Implementation	New York, NY	McGraw-Hill Education	978-0071701099

Referencias digitales			
Autor	Fecha de recuperación	Título del documento	Vínculo
Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short	29 de mayo de 2024	Cybersecurity Essentials	https://ebin.pub/cybersecurity-essentials-9781119362395-9781119362432-9781119362456-2018943782.html
Kevin D. Mitnick, William L. Simon	29 de mayo de 2024	The Art of Deception: Controlling the Human Element of Security	https://repo.zenk-security.com/Magazine%20E-book/Kevin_Mitnick_-_The_Art_of_Deception.pdf
Dafydd Stuttard, Marcus Pinto	29 de mayo de 2024	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws	https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Dafydd%2

			0Stuttard,%20Marcus%20Pinto%20-%20The%20web%20application%20hacker's%20handbook_%20finding%20and%20exploiting%20security%20flaws-Wiley%20(2011).pdf
William Stallings, Lawrie Brown	29 de mayo de 2024	Computer Security: Principles and Practice	https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/Computer_Security_Principles_and_Practice_(3rd_Edition).pdf
David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni	29 de mayo de 2024	Metasploit: The Penetration Tester's Guide	https://www.kea.nu/files/textbooks/humblesec/metasploit_apenetrationtestersguide.pdf