Programa de experiencia educativa

Licenciatura en Ingeniería de Ciberseguridad e Infraestructura de Cómputo, 2023

1. Área Académica

Económico Administrativa

2. Programa Educativo

Licenciatura en Ingeniería de Ciberseguridad e Infraestructura de Cómputo

3. Entidad(es) Académica(s)	4. Región(es)
Facultad de Estadística e Informática	Xalapa

5. Código	6. Nombre de la Experiencia Educativa
	Seguridad en Redes de Cómputo

7. Área de Formación del Modelo Educativo Institucional	8. Carácter
Área de Formación Disciplinar	Obligatorio

9. Agrupación curricular distintiva
Academia de Redes

10. Valores

Horas Teóricas	Horas Prácticas	Horas Otras	Total de horas	Créditos	Equivalencia (s)
2	3	0	75	7	Ninguna

11. Modalidad y ambiente de aprendizaje		12. Espacio	13. Relación disciplinaria	14. Oportunidades de evaluación
M: Curso - Taller	A: Presencial	IPA: Intraprograma Educativo	Multidisciplinario	Todas

15. EE prerrequisito(s)

Ninguna

16. Organización de los estudiantes en el proceso de aprendizaje

Máximo	Mínimo
30	10

17. Justificación articulada a la Fundamentación del plan de estudios

Las actividades cotidianas de las personas, en el ámbito familiar, social, escolar y laboral incluyen la transmisión de todo tipo de información a través de las redes de cómputo, por lo que las organizaciones deben establecer y aplicar políticas sobre el manejo de los datos al interior de su red, de forma que se pueda garantizar el acceso y uso adecuado de los mismos. La experiencia educativa Seguridad en Redes de Cómputo, permitirá al egresado identificar y llevar a la práctica distintas tecnologías que permiten la implementación de políticas de red que coadyuban a garantizar la calidad del servicio y la seguridad de la información que en ella circula.

18. Unidad de competencia (UC)

El estudiante aplica políticas de seguridad y de gestión de tráfico, a través de la configuración de distintos protocolos y tecnologías que permiten la manipulación de paquetes en dispositivos de red y de cómputo, de forma ética, responsable y colaborativa, con el fin de asegurar la disponibilidad, integridad y confidencialidad de los datos que circulan en una red de cómputo.

19. Saberes

Heurísticos	Teóricos	Axiológicos

• Comprensión de la necesidad de estrategias de seguridad en las redes de cómputo
• Comprensión del propósito de los diferentes tipos de ACL
• Configuración de políticas de seguridad en routers, a través de ACL estándar y extendidas
• Comprensión de los diferentes tipos de VPN.
• Configuración de VPN con distintos niveles de seguridad.
• Comprensión de los beneficios y fundamentos teóricos de la calidad de servicio.
	• Conceptos básicos de seguridad
	  ○ Triada CID
	  ○ Estados de los datos (en tránsito, almacenados y en proceso)
	  ○ Estrategias para la protección de los datos en tránsito (con base en hardware, con base en software, con base en la red)
	  ○ Políticas de ciberseguridad
	  ○ Mejores prácticas de seguridad en redes (VPN, Firewalls, IPS, etc.)
	• Listas de control de acceso
	  ○ Propósito
	  ○ Máscara wildcard
	  ○ Pautas para la creación de ACL
	  ○ ACL estándar (nombradas y numeradas)
		• Interés por el aprendizaje.
		• Curiosidad para comprender los fundamentos de la disciplina.
		• Creatividad en el diseño de soluciones.
		• Ética en el manejo de los datos.
		• Perseverancia en la resolución problemas.
		• Respeto por las opiniones de los demás.
		• Empatía con sus compañeros de grupo.
		• Responsabilidad en la entrega de evidencias
		• Trabajo colaborativo.

• Configuración de políticas de calidad de servicio en distintos dispositivos de red (virtuales o físicos). • Comprensión de las funciones y distintas tecnologías de firewalls. • Configuración de distintos tipos de filtrado de datos, a través de firewalls • Comprensión de los fundamentos teóricos sobre los sistemas de detección y prevención de intrusiones. • Configuración de sistemas de detección y prevención de intrusiones.	○ ACL extendidas (nombradas y numeradas) • Redes Privadas Virtuales (VPN) ○ Función y beneficios de las VPN ○ Tipos de VPN (sitio a sitio, acces remoto) ○ IPSec (tecnologías para encapsulación, confidencialidad, integridad, autenticación e intercambio seguro de llaves) • Calidad de Servicio (QoS) ○ Propoósito ○ Características del tráfico de red ○ Priorización del tráfico de red ○ Algoritmos de formación de colas (WFQ, CBWFQ, LLQ) ○ Modelos de QoS (servicio mínimo, servicios integrados y diferenciados) ○ Herramientas para implementación de QoS (clasificación, marcación y prevención de congestión) • Firewalls ○ Funciones ○ Tipos de firewalls ○ Tecnologías de firewall ○ Filtrado de paquetes ○ Filtrado por dirección ○ Filtrado por servicio • Sistemas de Detección y Prevención de Intrusiones (IDPS) ○ Funciones clave de las tecnologías IDPS ○ Metodologías comunes de detección de incidentes ○ Tecnologías IDPS (componentes y	

	arquitectura, capacidades de seguridad) o IDPS basados en red o IDPS basados en host	

20. Estrategias generales para el abordaje de los saberes y la generación de experiencia

	Actividad presencial	Actividad virtual
De aprendizaje	Lectura, síntesis e interpretación. Búsqueda de información. Discusiones grupales. Organizadores gráficos Estudio de casos. Resolución de prácticas.	Entrega oportuna de evidencias digitales (reportes, bitácoras, ejercicios, etc.)
De enseñanza	Discusión dirigida. Exposición con apoyo tecnológico variado. Definición de prácticas y casos de estudio Dirección de prácticas Organización de grupos colaborativos Retroalimentación de las actividades	

21. Apoyos educativos.

Libros Recursos de internet (páginas, videos, etc.) Software especializado (simuladores de red, analizador de paquetes, etc.). Computadora Proyector de video Pintarrón Plataforma educativa (Eminus, Cisco Netacad, Moodle, Teams, etc.)

22. Evaluación integral del aprendizaje.

Evidencias de desempeño por productos	Indicadores generales de desempeño	Procedimiento(s), técnica(s) e instrumento(s) de evaluación	Porcentaje

Exámenes (parciales o finales).	Resolución correcta de reactivos.	Rúbrica	45%
Reportes de investigación	Entrega en tiempo y forma Redacción clara y coherente.	Rúbrica	10%
Documentación del proyecto final	Entrega en tiempo y forma Redacción clara y coherente.	Rúbrica	10%

Evidencias de desempeño por demostración	Indicadores generales de desempeño	Procedimiento(s), técnica(s) e instrumento(s) de evaluación	Porcentaje
Resolución de prácticas	Solución correcta Apego al procedimiento	Rúbrica	20%
Presentación del Proyecto final.	Entrega oportuna, correcta y funcional.	Rubrica	15%

23. Acreditación de la EE

El estudiante deberá presentar con suficiencia cada una de las evidencias de desempeño para cualquiera de las evaluaciones finales (ordinario, extraordinario o título de suficiencia), así como cumplir con los porcentajes de asistencia que marca el estatuto de alumnos.

24. Perfil académico del docente

Licenciado en Informática, Licenciado en Redes y Servicios de Cómputo o carrera afín, con estudios de posgrado, con cursos de formación o experiencia profesional en el área de ciberseguridad en redes de cómputo de al menos un año, con experiencia docente de al menos 2 años en el nivel superior y cursos de formación pedagógica.

25. Fuentes de información

Cisco Systems. Programa Cisco Netacad CCNA v7 (2 de agosto del 2022). Enterprise networking security and automation. https://www.netacad.com/

Cisco Networking Academy (2020). Enterprise Networking, Security, and Automation Companion Guide (Ccnav7). Cisco Press.

Zwicky, E., Cooper, S. & Chapman D. (2000). Building Internet Firewalls, 2nd Edition. O'Reilly Media, Inc.
Stewart, J., Kinsey, D. (2020). Network Security, Firewalls, and VPNs, 3rd Edition. Johns & Bartlett Learning.
Froom, R., Flannagan, M. & Turek, K. (2008). Cisco Catalyst QoS: Quality of Service in Campus Networks. Cisco Systems
Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST Special Publication (SP) 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

26. Formalización de la EE

Fecha de elaboración	Fecha de modificación	Cuerpo colegiado de aprobación
Agosto de 2022		

27. Nombre de los académicos que elaboraron/modificaron

Martha Elizabet Domínguez Bárcenas, Angélica Pérez Hernández