DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		2			
SEMESTRE/ MÓDULO		4			
UNIDAD CURRICULAR		Seguridad en Redes de Computadoras			
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	Nº Resolución de la DGETP	Exp. Nº	Res. Nº	Acta Nº	Fecha __/__/____

Objetivos:

El objetivo de este curso es introducir al estudiante en los conceptos básicos de la seguridad informática de redes de datos TCP/IP.

Resultados de aprendizajes:

Incorpora conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir una red de datos TCP/IP

Establece los mecanismos de protección adecuados.

Saberes estructurantes de la unidad curricular:

1. Problemas de Seguridad de los protocolos TCP/IP
    a) Autenticación del origen (IP spoofing).
    b) Interacción IP/MAC, ARP spoofing.
    c) Ataques a protocolo de ruteo, ICMP.
    d) TCP session Hijacking, SYN Flooding.
    e) Capa de Aplicación: Servicio DNS.
    f) VLAN
2. Redes inalámbricas (WiFi):
    a) Requerimientos de seguridad (autenticación, control de acceso, confidencialidad, integridad).
    b) WEP, WPA, WPA2, EAP, 802.1X
3. Seguridad IP (IPSec):
    a) Asociaciones de Seguridad (SA).
    b) Modos de funcionamiento (túnel y transporte).
    c) Protocolo AH y ESP (encabezados y servicios que ofrecen).
    d) IPSec Key Management (IKE).
    e) IPsec y filtrado.
4. VPN
    a) ¿Qué es una VPN? VPN sobre Internet.
    b) Implementación de VPN.
5. Firewalls
    a) Definición. ¿Qué puede hacer y qué NO un firewall?.
    b) Filtrado de paquetes, con y sin estados. Generando reglas de filtrado.

c) Logging.

d) Arquitecturas de Firewall.

e) Tipos de Firewall.

f) Servicios Proxy y NAT.

6. Sistemas de detección y prevención de intrusiones (IDS/IPS):

a) Definición.

b) Clasificación y formas de detección.

c) Falsos positivos y negativos.

d) ¿Acciones automáticas? Dónde monitorizar (sensar).

e) Otro tipo de sensores (honeypots).

7. Diseño de un perímetro seguro:

a) Identificación de activos a proteger.

b) Identificación de fronteras.

c) Separación e identificación de zonas de seguridad.

Bibliografía:

Básica:

Gollman, Dieter (2009), Computer Security, Wiley Computing Publishing, 3rd. Editon.

Complementaria:

Garfinkel, S.; Spafford, G. & Schuartz, A. (2003); Practical Unix & Internet Security; Ed. O'Reilly; 3rd Edition.

Edney, J.; Arbaugh, W. (2004); Real 802.11 Security - Wi-Fi Protected Access and 802.11i. Addison-Wesley, 2004.

Zwicky, E.; Cooper, S. & Chapman, B. (2000); Building Internet Firewalls; Ed. O'Reilly; 2nd Editon