



**PROGRAMA PLANEAMIENTO EDUCATIVO
DEPARTAMENTO DE DISEÑO Y DESARROLLO CURRICULAR**

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		049	Educación Media Tecnológica		
PLAN		2004	2004		
SECTOR DE ESTUDIO		620	Informática		
ORIENTACIÓN		48S	Informática Énfasis Desarrollo y Soporte		
MODALIDAD		-	Presencial		
AÑO		3ro.	Tercero		
TRAYECTO		-	-		
SEMESTRE		-	-		
MÓDULO		-	-		
ÁREA DE ASIGNATURA		786	Taller de Mantenimiento Informático		
ASIGNATURA		37056	Redes de Datos y Seguridad		
ESPACIO o COMPONENTE CURRICULAR		Tecnológico			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 4	Cantidad de semanas: 32	
Fecha de Presentación: 14/09/2018	Nº Resolución del CETP	Exp. Nº	Res. Nº	Acta Nº	Fecha __/__/__

FUNDAMENTACIÓN

Las redes de datos se emplean más de lo que cualquiera hubiera imaginado, el modo en que se producen las interacciones sociales, comerciales, y personales cambia en forma continua para estar al día con la evolución de esta globalización. Mientras los desarrolladores empujan los límites de lo posible, las capacidades de las redes tendrán una función cada vez más importante para el éxito de esos proyectos. Para atender las nuevas circunstancias que implican estos cambios se requieren técnicos preparados y capacitados, para seguir la evolución del cambio constante.

¿Entendemos cómo realmente funciona Internet y cuál es la función de los ISP?.

Trabajar sobre Internet y no entender sus protocolos fundamentales, se considera algo realmente muy importante y es ahí donde se plantea el estudio de los protocolos dinámicos de redes de datos.

Conocer las características de un: “Core” ISP y como llegar a él, es algo muy importante, si entendemos que la información en la “cloud” (nube) es fundamental para todos.

Por otra parte, las empresas están cada vez más interconectadas y necesitan un 100% de la misma, es ahí donde la correcta configuración de Protocolos Dinámicos comienza a jugar el papel más importante, la conectividad 24x7. Dichos protocolos nos van a permitir seguridad de acceso a las herramientas de Internet y Corporativas, en un mundo cada vez más conectado.

Toda organización pública o privada, nacional o internacional, independientemente de su sector, tiene una gran dependencia de su infraestructura informática en un mundo altamente conectado. En la actualidad ya es un hecho que la Seguridad Informática y la protección de datos, han dejado de ser una tarea más de los profesionales de TI, para transformarse en una disciplina crítica de alta especialización.

Este curso lo capacita para analizar y entender los riesgos existentes ante hechos fortuitos y ataques en un ambiente de redes, permitiendo detectar sus vulnerabilidades. Estudia los tipos y formas de daños o ataques que pueden producirse en sistemas de servidores y su entorno físico. Propone una metodología de planes de contingencia para prevenir, detectar, contener o mitigar la materialización de estos riesgos y poder restaurar los servicios que se vieron afectados.

La Seguridad de la Información es un aspecto muy importante en el mundo de hoy. Los principales medios de comunicación se repiten los ataques de virus, hackers y otros peligros tecnológicos. Desde el ámbito corporativo y gubernamental, la búsqueda de profesionales en Seguridad Informática se ha duplicado y la tendencia sigue creciendo.

Las auditorías de red, son un punto muy importante para cualquier organización que trabaje sobre equipos de redes informáticos, siendo un factor no solamente importante, sino que necesario.

Dichas auditorías logran el conocimiento sobre la seguridad en redes TCP/IP, trabajar con ejercicios prácticos empleando herramientas de red. Familiarización con los comandos y herramientas más comunes para poder ser empleadas en auditorías de sistemas y redes.

En general, todas estas herramientas para auditorías son herramientas de seguridad y hacking. Se utilizan para fines tanto legales como ilegales, están diseñadas para ayudar a los administradores y profesionales de seguridad a asegurar las redes y los sistemas de información.

OBJETIVOS

Esta asignatura profundiza los conocimientos adquiridos por el alumno en el diseño e implementación de soluciones en redes de datos LAN y WAN en base a las normas y estándares vigentes de la industria. Se profundiza en el estudio de los protocolos de ruteo de paquetes en las redes de datos privadas e Internet.

Enrutamiento se refiere al proceso en el que los enrutadores aprenden sobre redes remotas, encuentran todas las rutas posibles para llegar a ellas y luego escogen las mejores.

En otras palabras, los enrutadores deciden después de examinar la dirección IP de destino, dónde enviar los paquetes, para que eventualmente lleguen a su red de destino.

Nuestro principal objetivo es comprender los estados de los routers en su operación dinámica en las distintas topologías de “Core” de una red de datos.

El curso prepara en aspectos de Seguridad, para desempeñarse en puestos de administración y monitoreo de la defensa de infraestructuras de TI.

A.N.E.P.
Consejo de Educación Técnico Profesional

Analizar y entender los riesgos existentes ante distintos ambientes de las Redes de Datos, estudiando los tipos de ataques y daños colaterales.

Proponer metodologías para mitigar eventos no deseados en informática, desde el punto de vista de la seguridad.

Diseñar una Auditoria de la red, para obtener un mejor conocimiento de la misma y saber cómo proceder ante ataques.

CONTENIDOS:

El contenido del curso se desarrollará en base a las siguientes unidades temáticas.

Unidad 1: Protocolos capa de Transporte

Tiempo sugerido 12 horas

TCP Protocolo con conexión

Cabecera TCP, detección de errores, acuse de recibo, Transporte confiable,

Saludo de tres vías

Por qué se utiliza un búfer en la comunicación de datos

Protocolos de ventana deslizante

Administración de conexiones

UDP Protocolo sin conexión

Usos del UDP

Diferencias entre UDP y TCP

Control de Acceso al medio

Prácticas recomendadas

1.1 Analizar una comunicación, usando “Analizador de Protocolos”.

Unidad 2: Protocolos capa de Aplicación

Tiempo sugerido 12 horas

Configuración de server en capa Aplicación

Protocolo de Resolución de Direcciones (DHCP)

Protocolo de encaminamiento: SMTP

Protocolos de entrega final: POP e IMAP

Login remoto: telnet, rlogin , ssh.

Transferencia de ficheros: FTP y TFTP

Unidad 3: Convergencia en Redes.

Tiempo sugerido 20 horas

Concepto de convergencia de redes de datos.

Tabla de ruteo - Ruteo en VLAN (ver caso de vrf).

Ruteo Dinámico y estático, des el punto de vista de Convergencia.

Uso de VLAN y Configuración en SW y Router

Concepto de VPN capa2 y VPN capa3

NAT

VPN privadas y públicas

Servicios en Cloud (nube) y su tendencia.

Unidad 4: Enrutamiento Estático.

Tiempo sugerido 12 horas

Concepto de Vlsn

Concepto de ruteo estático.

Definición de “peso en rutas”.

Configuración de uso de rutas en sistema de backup y su convergencia en redes ante eventos.

Prácticas recomendadas

- 4.1 Ruteo estático utilizando redes, con Simuladores de Red.
- 4.2 Ruteo estático utilizando subredes, con Simuladores de Red.
- 4.3 Ruteo estático utilizando subredes VLSM, con Simuladores de Red.

Unidad 5: Ruteo dinámico.

Tiempo sugerido 24 horas

Concepto de Vector distancia y Estado de Enlace

Loop de enrutamiento.

Estudios de casos de loop .

Características de Protocolos IGP y de Protocolos EGP y su aplicación.

Prácticas recomendadas

- 5.1 RIP, OSPF.
- 5.2 Configuración de servicio DHCP.
- 5.3 Configuración de servicio Router, switch y redes Wifi.

Unidad 6: Equipos de ruteo de última generación.

Tiempo sugerido 8 horas

Estudiar distintos equipos de última generación que se presentan actualmente, no se define cuáles deben ser, porque debe buscarse la inquietud del grupo y del propio docente en la propuesta.

Proponer trabajo grupal de arquitectura de equipos de última generación.

Unidad 7: Amenazas Informáticas

Tiempo sugerido 20 horas

Amenazas informáticas externas e internas (uso de dispositivos personales).

Técnicas de mantenimiento preventivo.

Protección contra software mal intencionado.

Tipos de malware y ataques TCP/IP.

Técnicas de seguridad.

Distintos tipos de Firewall y Proxy.

Reglas de seguridad. Concepto de seguridad detección automática de ataques.

Housing y sus características en las corporaciones desde la Seguridad.

Prácticas recomendadas

7.1 Analizar una red, usando herramientas de software libre (tcpdump).

7.2 Crear reglas de Seguridad Access-List y aplicación en Firewall.

7.3 Implementación de una red cliente servidor, para estudio de Seguridad.

Unidad 8: Auditorias

Tiempo sugerido 20 horas

Riesgos existentes y como detectar vulnerabilidades en la red.

Herramientas que describiremos a continuación son herramientas de seguridad y hacking: Nmap; Nessus; Wireshark; NetStumbler, tcpdump, Netflow.

Manejo de daños en la red. Y Planes de Contingencia (backup de información) y copias de seguridad.

Redes Wifi y su Seguridad en las Auditorias.

Diseñar Política de Seguridad

Prácticas recomendadas

8.1 Auditorias de red, realizando un estudio de un Caso Real.

PROPUESTA METODOLÓGICA

El curso se desarrollará en módulos de cuatro horas semanales, la carga horaria propuesta abarca 128 horas de clases, donde se implemente los distintos protocolos trabajados en clase, explorando la convergencia de la red, backup y servicios implementados. También se abarca temas de Seguridad Informática. Se recomienda el estudio en grupo y puesta en marcha de los protocolos estudiados en la clase.

Aspectos teóricos

El curso está planteado para profundizar en el plano teórico lo necesario para comprender adecuadamente los temas abordados

Estos temas forman una unidad por lo que el plano teórico es uno de sus componentes ineludibles, y este criterio también abarca el plano práctico.

EQUIPAMIENTO, HERRAMIENTAS Y MATERIALES NECESARIO.

Equipamiento informático y de Red del Salón

Cantidad	DESCRIPCIÓN
15	PCs (alumnos) de última generación en correcto funcionamiento (a partir de generación Intel Core i5).
1	PC (docente) de última generación en correcto funcionamiento (a partir de generación Intel Core i5) con capacidad para el manejo de máquinas virtuales.
1	Red operativa para 20 puestos de red con conexión a Internet, según normas de cableado estructurado con su correspondiente Mini-Rack de red (9U).

Equipamiento de Red, y otros

Cantidad	DESCRIPCIÓN
3	Con prestaciones de: configuración de subinterface. configuración de prestación de ruteo virtual (vrf)

A.N.E.P.
Consejo de Educación Técnico Profesional

	access-list, configuración de línea de seguridad. puerto Ethernet 10/100 y dos 10/100/1000. cli de comandos. protocolo SNMP para gestión de monitoreo.
4	Switch con prestaciones de: configuración de vlan configuración de línea por comandos cli gestión remota y protocolo SNMP mínimo 8 puertos, puerto Ethernet 10/100 puertos y dos 10/100/1000, puertos eléctricos.
1	Router Wifi.con prestaciones de: configuración de remota manejo de distintos canales de frecuencia,
1	Rack de datos
1	Analizador de red

EVALUACIÓN

Consta de tres evaluaciones en el año, dos evaluaciones teóricas y una prueba práctica.

Para llegar a dicho fin, se plantea:

Realización de dos Parciales en el año.

Prácticas sobre Protocolos trabajados en clase.

Proyecto de pasaje de grado con su correspondiente defensa grupal e individual.

Materiales necesarios

Tres Routers, con prestaciones de:

configuración de subinterface.

configuración de prestación de ruteo virtual (vrf)

access-list, configuración de línea de seguridad.

puerto Ethernet 10/100 y dos 10/100/1000.

cli de comandos.

protocolo SNMP para gestión de monitoreo.

Cuatro Switch con prestaciones de:

configuración de vlan

configuración de línea por comandos cli

gestión remota y protocolo SNMP

mínimo 8 puertos, puerto Ethernet 10/100 puertos y dos 10/100/1000, puertos eléctricos.

Router Wifi.con prestaciones de:

configuración de remota

manejo de distintos canales de frecuencia,

Rack de Datos

Analizadores de red (software)

Diez PC, cada 20 alumnos.

BIBLIOGRAFÍA

Libro 1 Networking de Ciscopress (Autor Vito Amato) isbn 1-57870-218-6

Libro 2 Networking de Ciscopress (Autor Vito Amato) isbn 1-58713-002-5

Redes de Computadoras – Andrés Tanembaun

Organización de computadoras un enfoque estructurado.

Seguridad Informática Hacking Ético. Conocer el ataque para una mejor defensa.
(Autor ACISSI - Damien BANCA).

Ataques en Redes de Datos IPV4 e IPV6. (Garcia Rambla, Juan Luis).