I. INFORMACIÓN GENERAL

CURSO	:	Seguridad De Servicios De Red
CÓDIGO	:	RC61
CICLO	:	201700
CUERPO ACADÉMICO	:	**Seminario García, Hernán Augusto**
CRÉDITOS	:	3
SEMANAS	:	9
HORAS	:	6 H (Teoría) Semanal
ÁREA O CARRERA	:	Ingenieria de Redes y Comunicaciones Epe

II. MISIÓN Y VISIÓN DE LA UPC

Misión: Formar líderes íntegros e innovadores con visión global para que transformen el Perú.

Visión: Ser líder en la educación superior por su excelencia académica y su capacidad de innovación.

III. INTRODUCCIÓN

El presente es un curso de especialidad de la carrera Ingeniería de Redes y Comunicaciones EPE, de carácter teórico, dirigido a los estudiantes del nivel 6 de la carrera, que busca desarrollar la competencia general de pensamiento innovador nivel 2 y la competencia específica E - Capacidad para identificar, formular y resolver problemas en Ingeniería de Redes y Comunicaciones - nivel 2.

Este curso permitirá al alumno analizar técnicas y herramientas necesarias para proteger los servicios de una empresa, considerando soluciones en hardware y software. Se tocaran temas como: diseño de políticas de seguridad y su aplicación utilizando herramientas como: proxy, firewall, filtros de contenido, IDS, IPS, VPN, criptografía, entre otras.

IV. LOGRO (S) DEL CURSO

Al finalizar el curso el alumno será capaz de comprender el diseño, la implementación, operación y mantenimiento de la Seguridad Informática que requieren los Servicios de Red de una empresa, aplicando técnicas, herramientas y metodologías internacionales relacionadas.

V. UNIDADES DE APRENDIZAJE

UNIDAD Nº: 1 Seguridad en la infraestructura y conectividad de red

LOGRO

El alumno al finalizar la unidad será capaz de aplicar conceptos básicos sobre la seguridad en los componentes de red.

TEMARIO

Directivas y procedimientos relacionados con la seguridad

Seguridad en la topología de red
Seguridad en la infraestructura
Dispositivos de Seguridad en la red
Acceso remoto seguro

HORA(S) / SEMANA(S)
SES 1 y 2

UNIDAD Nº: 2 Protección de las redes

LOGRO
El alumno al finalizar la unidad será capaz de aplicar conceptos para detectar, controlar y diagnosticar la seguridad de las redes.

TEMARIO
Control y diagnóstico de redes
Sistemas de detección de intrusiones
Conexiones seguras a Internet
Amenazas y vulnerabilidades tecnológicas
Tipos de ataques a redes

HORA(S) / SEMANA(S)
SES 3 y 4

UNIDAD Nº: 3 Control

LOGRO
El alumno al finalizar la unidad será capaz de aplicar conceptos sobre el control de acceso y sistemas de autenticación segura.

TEMARIO
Introducción al control de acceso
Métodos de control de acceso
Modelos de control de acceso a la información
Conectividad de acceso remoto
Servicios de Autenticación
Prácticas de control de acceso

HORA(S) / SEMANA(S)
SES 5 A 7

UNIDAD Nº: 4 Seguridad de los servicios de red

LOGRO
El alumno al finalizar la unidad será capaz de aplicar conceptos de seguridad sobre los principales servicios de la red

TEMARIO
Seguridad en las comunicaciones
Seguridad del correo electrónico

Seguridad en la web
Seguridad del sistema operativo
Seguridad de las aplicaciones

HORA(S) / SEMANA(S)
SES 8 A 9

UNIDAD Nº: 5 Criptografia

LOGRO
El alumno al finalizar la unidad será capaz de aplicar conceptos para la protección y cifrado de la información.

TEMARIO
Introducción a la criptografía
Algoritmos criptográficos
Sistemas criptográficos
Estándares y protocolos de la criptografía
Infraestructura de clave pública (PKI)

HORA(S) / SEMANA(S)
SES 10 A 11

UNIDAD Nº: 6 Administración de la Seguridad de Red

LOGRO
El alumno al finalizar la unidad será capaz de aplicar conceptos y buenas prácticas para operar y administrar la infraestructura y los componentes de seguridad de la red.

TEMARIO
Gestión de eventos de seguridad
Gestión de incidentes de seguridad
Gestión de vulnerabilidades tecnológicas
Auditorías de seguridad

HORA(S) / SEMANA(S)
SES 12 A 14

VI. METODOLOGÍA

El curso se dicta en 14 sesiones teóricas y 1 sesión de evaluación final, en las clases se desarrollan conceptos e ideas que deben ser corroborados con ejercicios y casos prácticos, se promueve la participación activa del alumnado, se realizan discusiones y solución de problemas.

VII. EVALUACIÓN

FÓRMULA

20% (PC1) + 30% (TB1) + 20% (PC2) + 30% (TF1)

TIPO DE NOTA	PESO %
PC - PRÁCTICAS PC	20
TB - TRABAJO	30
PC - PRÁCTICAS PC	20
TF - TRABAJO FINAL	30

VIII. CRONOGRAMA

Módulo Regular

TIPO DE PRUEBA	DESCRIPCIÓN NOTA	NÚM. DE PRUEBA	FECHA	OBSERVACIÓN	RECUPERABLE
PC	PRÁCTICAS PC	1	Ses 6	Individual - Unidades 01 y 02	SÍ
TB	TRABAJO	1	Ses 8	Grupal - Unidades 01 y 02	NO
PC	PRÁCTICAS PC	2	Ses 12	Individual - Unidades 03 a 05	SÍ
TF	TRABAJO FINAL	1	Ses 15	Grupal - Unidades 01 a 05	NO

IX. BIBLIOGRAFÍA DEL CURSO

BÁSICA

TANENBAUM Andrew S.Wetherall, David J. y ROMERO ELIZONDO, Alfonso Vidal (2012) Redes de computadoras. México, D.F. : Pearson Educación.
(004.6 TANE 2012)

RECOMENDADA

(No necesariamente disponible en el Centro de Información)

TIPTON Harold F., y KRAUSE, Micki, (2009) Information security management handbook. Boca Raton, Florida : Auerbach.
(005.8 TIPT)