TÉCNICO SUPERIOR UNIVERSITARIO EN TECNOLOGÍAS DE LA INFORMACIÓN ÁREA INFRAESTRUCTURA DE REDES DIGITALES EN COMPETENCIAS PROFESIONALES

ASIGNATURA DE CIBERSEGURIDAD

1. Competencias	Desarrollar soluciones tecnológicas mediante la aplicación de fundamentos de programación y redes que atiendan necesidades de las organizaciones.
2. Cuatrimestre	Quinto
3. Horas Teóricas	24
4. Horas Prácticas	66
5. Horas Totales	90
6. Horas Totales por Semana Cuatrimestre	6
7. Objetivo de aprendizaje	El alumno realizará tareas para monitorear, analizar, detectar y responder a posibles amenazas de ciberseguridad a través de herramientas y metodologías de aseguramiento de redes.

Unidades de Aprendizaje		Horas		
		Teóricas	**Prácticas**	**Totales**
I.	**Introducción a Ciberseguridad y Sistemas Operativos.**	4	8	12
II.	**Protocolos, Servicios, Infraestructura y Principios de Seguridad de Redes**	8	16	24
III.	**Monitoreo y Protección de Redes y Dispositivos Finales**	4	14	18
IV.	**Criptografía e Infraestructura de clave pública**	4	14	18
V.	**Análisis de Intrusión y Manejo de Incidentes.**	4	14	18
	Totales	**24**	**66**	**90**

CIBERSEGURIDAD

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**I. Introducción a Ciberseguridad y Sistemas Operativos**
2. Horas Teóricas	4
3. Horas Prácticas	8
4. Horas Totales	12
5. Objetivo de la Unidad de Aprendizaje	El alumno ejecutará operaciones básicas y tareas relacionadas con seguridad en ambientes Linux y Windows, para realizar análisis de ciberseguridad.

Temas	Saber	Saber hacer	Ser
Ciberseguridad y el Centro de Operaciones de Seguridad (SOC)	Identificar los conceptos principales de ciberseguridad. Describir las funciones del Centro de Operaciones de Seguridad (SOC).		Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico
Sistema Operativo Windows	Identificar los procesos que habilitan la operación del sistema operativo Windows. Identificar las herramientas que aseguran dispositivos finales con sistema operativo Windows.	Inspeccionar procesos, hilos y registros que se ejecutan en la PC	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico
Sistema Operativo Linux	Explicar las características y componentes del sistema operativo Linux Identificar comandos básicos que interactúan con el sistema operativo Linux	Ejecutar operaciones básicas en el sistema operativo Linux así como tareas relacionadas con seguridad y administración.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico

CIBERSEGURIDAD

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Realiza un proyecto que contiene un prototipo y un reporte con base en un caso de estudio final que incluya: Reporte • Lista de elementos de la topología que se derive del caso de estudio. • Diagrama de conexiones entre dispositivos. • Tabla de direccionamiento IP para los diferentes dispositivos de la topología. • Lista de pasos realizados para asegurar la(s) PC(s) con sistema operativo Windows. • Lista de pasos realizados para configurar y asegurar la(s) PC(s) con sistema operativo Linux. • Lista de pruebas de acceso y seguridad realizadas a los dispositivos de la topología. • Resumen de la información de configuración del(los)	1. Identificar los conceptos básicos de Ciberseguridad. 2. Comprender la operación y tareas básicas para interactuar con sistemas operativos Windows y Linux. 3. Comprender los procesos y herramientas utilizadas para asegurar dispositivos con sistemas operativos Windows y Linux. .	-Estudio de caso -Lista de cotejo

Host(s) Virtualizados de acuerdo al caso de estudio final. Prototipo • Conexión a Internet. • PC(s) con sistema operativo Windows. • PC(s) con sistema operativo Linux. • Host(s) Virtualizados • Switch • Router • Conexión a Internet		

CIBERSEGURIDAD

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Prácticas de laboratorio -Práctica guiada -Análisis de casos	Analizador de tráfico de red Simulador de redes Software para virtualizar Distribuciones de sistemas operativos abiertos y propietarios Switches Routers Equipo audiovisual Equipo de cómputo Internet

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X	X	

CIBERSEGURIDAD

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**II. Protocolos, Servicios, Infraestructura y Principios de Seguridad de Redes**
2. Horas Teóricas	8
3. Horas Prácticas	16
4. Horas Totales	24
5. Objetivo de la Unidad de Aprendizaje	El alumno operará herramientas de monitoreo para identificar ataques contra protocolos y servicios de red.

Temas	Saber	Saber hacer	Ser
Protocolos y Servicios de Red	Identificar el conjunto de protocolos TCP/IP y los servicios asociados que permiten la ejecución de tareas en la red.	Realizar análisis de tramas Ethernet por medio de software de captura de tráfico. Verificar la comunicación TCP/IP de tres vías entre clientes y servidores con software de captura de tráfico Verificar las características del tráfico TCP y UDP con software de captura de tráfico.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico
Infraestructura de Red	Identificar los componentes de la infraestructura de redes tanto alámbrico como inalámbrico. Explicar la operación de la infraestructura de redes, incluyendo la seguridad y el diseño.	Verificar la conectividad local y las pruebas a la seguridad de redes basadas en listas de control de acceso. Verificar en software de simulación de redes las trayectorias de paquetes en topologías LAN y WAN.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico

Temas	Saber	Saber hacer	Ser
Fundamentos de Seguridad de Redes	Identificar herramientas y métodos utilizados por hackers para realizar ataques de redes. Identificar las características de los diferentes tipos de ataques utilizados por Hackers: Reconocimiento, Acceso, Ingeniería Social y Denegación de Servicio.	Seleccionar herramientas de monitoreo de redes para identificar ataques contra protocolos y servicios.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico.
Ataques de Redes	Identificar las vulnerabilidades de protocolos y servicios de red que incluyen, IP, TCP, UDP, ARP, DNS, DHCP, HTTP y E-mail.	Realizar la exploración de Peticiones y Mensajes de Respuesta DNS con software de captura de tráfico. Verificar las características de ataques de inyección contra bases de datos SQL a partir de archivos PCAP.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico

CIBERSEGURIDAD

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Realiza un proyecto que contiene un prototipo y un reporte con base en un caso de estudio que incluya: **Reporte** • Capturas de pantallas de las tramas Ethernet con la interpretación de los principales campos, obtenidas de la ejecución del software analizador de protocolos. • Capturas de pantallas de los segmentos TCP/IP identificando los campos que caracterizan las etapas de la negociación del "saludo de tres vías", obtenidas de la ejecución del software analizador de protocolos. • Lista de pruebas a la seguridad basadas en listas de control de acceso, realizadas a la topología construida en el caso de estudio. • PC(s) con sistema operativo Windows. • PC(s) con sistema operativo Linux. • Host(s) Virtualizados	1. Identificar los protocolos y servicios de TCP/IP. 2. Identificar los componentes de la infraestructura de red. 3. Comprender la operación de la infraestructura de red. 4. Identificar características de diferentes tipos de ataques. 5. Identificar herramientas y métodos utilizados para realizar ataques de red.	-Estudio de caso -Lista de cotejo

• Switch. • Router. • Conexión a Internet.		

CIBERSEGURIDAD

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Prácticas de laboratorio -Práctica guiada -Análisis de casos	Material didáctico en línea especializado en redes. Equipo audiovisual o video proyección. Pintarrón. Software simulador de redes. Software analizador de tráfico en redes de datos. Computadora.

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X	X	

CIBERSEGURIDAD

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**III. Monitoreo y Protección de Redes y Dispositivos Finales**
2. Horas Teóricas	4
3. Horas Prácticas	14
4. Horas Totales	18
5. Objetivo de la Unidad de Aprendizaje	El alumno implementará en ambientes controlados la infraestructura para monitoreo y protección de redes y dispositivos finales.

Temas	Saber	Saber hacer	Ser
Protección de la Red	Identificar propuestas que establecen defensas de seguridad de redes, métodos de control de acceso y análisis de ciberseguridad como base de la inteligencia contra amenazas.	Seleccionar el medio de transmisión y protocolos de comunicación con base en el entorno de red específico.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico
Análisis y Seguridad de Dispositivos Finales	Identificar las amenazas a los dispositivos finales y los métodos para protegerlos de los ataques.	Elaborar topologías físicas de redes de área local y amplia, así como diagramas de la estructura de la trama genérica.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico

Temas	Saber	Saber hacer	Ser
Monitoreo de Seguridad.	Identificar las tecnologías de seguridad y archivos de registro utilizados en el monitoreo de redes.	Verificar el tráfico de redes por medio de agentes que recolectan información en el servidor con Netflow y software de simulación. Verificar los datos generados en las redes utilizando Syslog, registros de accesos de usuarios por medio de AAA, servidores con Netflow y software de simulación.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico

CIBERSEGURIDAD

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Realiza un proyecto que contiene un prototipo y un reporte con base en un caso de estudio que incluya: **Reporte** • Captura de pantallas con la verificación en software de simulación del tráfico de la red que represente la topología del caso de estudio recolectando información con un servidor de captura NETFLOW. **Prototipo** • Topología, basada en el caso de estudio, modelada en software de simulación de redes.	1. Identificar métodos de control de acceso y análisis de ciberseguridad. 2. Identificar amenazas y métodos de protección a dispositivos finales. 3. Comprender tecnologías utilizadas para el monitoreo de redes.	-Estudio de caso -Lista de cotejo

CIBERSEGURIDAD

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Prácticas de laboratorio -Práctica guiada -Análisis de casos	Analizador de tráfico de red Simulador de redes Software para virtualizar Distribuciones de sistemas operativos abiertos y propietarios Switches Routers Equipo audiovisual Equipo de cómputo Internet

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

CIBERSEGURIDAD

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**IV. Criptografía e Infraestructura de clave pública**
2. Horas Teóricas	4
3. Horas Prácticas	14
4. Horas Totales	18
5. Objetivo de la Unidad de Aprendizaje	El alumno implementará técnicas criptográficas para mantener la confidencialidad e integridad de los datos.

Temas	Saber	Saber hacer	Ser
Principios de Criptografía	Describir las características de las bases criptográficas de privacidad y seguridad de los datos.	Elaborar cifrado de datos en Open SSL y herramientas de Hackeo.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico
Integridad y Autenticación de origen.	Describir las técnicas que preservan la privacidad y seguridad de los datos.	Elaborar Hashes en Open SSL. Verificar Hashes en Open SSL.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico
Confidencialidad	Describir las características de las técnicas de cifrado en la confidencialidad a los datos.		Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico

Temas	Saber	Saber hacer	Ser
Infraestructura de Clave Pública	Identificar los componentes que permiten habilitar infraestructuras de clave pública.	Validar los certificados de confianza de los navegadores de internet. Verificar en escenarios virtuales las características de ataques Man-In-The-Midle.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico

CIBERSEGURIDAD

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Realiza un proyecto que contiene un prototipo y un reporte con base en un caso de estudio que incluya: **Reporte** • Lista de pasos del procedimiento para realizar encriptación de datos utilizando Open SSL en la(s) PC(s) con sistema operativo Linux, que conforme(n) parte de la Topología construida del caso de estudio final. • Lista de pruebas para validar los certificados de confianza de los navegadores de internet que pertenezcan a la(s) PC(s) y que formen parte de la topología construida del caso de estudio final. Prototipo • PC(s) con sistema operativo Windows**.** • PC(s) con sistema operativo Linux. • Host(s) Virtualizados. • Switch. • Router. • Conexión a Internet	1. Comprender los principios de criptografía. 2. Identificar técnicas para preservar la privacidad y seguridad de los datos. 3. Comprender algoritmos de cifrado para proporcionar confidencialidad a los datos. 4. Identificar componentes que habilitan la infraestructura de clave pública.	-Estudio de caso -Lista de cotejo

CIBERSEGURIDAD

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Prácticas de laboratorio -Práctica guiada -Análisis de casos	Analizador de tráfico de red Simulador de redes Software para virtualizar Distribuciones de sistemas operativos abiertos y propietarios Switches Routers Equipo audiovisual Equipo de cómputo Internet

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X	X	

CIBERSEGURIDAD

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**V. Análisis de Intrusión y Manejo de Incidentes**
2. Horas Teóricas	4
3. Horas Prácticas	14
4. Horas Totales	18
5. Objetivo de la Unidad de Aprendizaje	El alumno operará conjuntos de herramientas de seguridad para analizar, detectar y reportar eventos de intrusión.

Temas	Saber	Saber hacer	Ser
Análisis de Intrusión de Datos	Identificar las herramientas de detección de ataques de recolección de alertas. Identificar herramientas empresariales en la gestión de archivos de seguridad de redes (NSM).	Controlar la comunicación entre Hosts internos de una red y servidores de Malware Utilizando Firewalls y Sistemas de Detección de Intrusos (IDS) Realizar la normalización de la información contenida en archivos de bitácora SYSLOG Realizar la detección de transferencias de archivos posiblemente infectados a partir de archivos PCAP.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico
Modelos de Respuesta a Incidentes	Identificar las características de los modelos de respuesta a incidentes.		Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico

Temas	Saber	Saber hacer	Ser
Manejo de Incidentes	Identificar las características principales de la norma NIST 861-R2.	Elaborar reportes de manejo de ataques basados en los modelos más comunes de respuesta a incidentes.	Observador Analítico Sistemático Hábil para interpretar información Proactivo Lógico

CIBERSEGURIDAD

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Realiza un proyecto que contiene un prototipo y un reporte con base en un caso de estudio que incluya: Reporte • Lista de pasos del procedimiento para configurar el control anti-malware utilizando reglas de firewall y sistemas de detección de intrusos en una(s) PC(s) ya sea con sistema operativo Windows o Linux. • Lista de pruebas para detectar transferencias de programas con malware a partir de un archivo PCAP, obtenido de la topología construida del caso de estudio final. Prototipo • PC(s) con sistema operativo Windows**.** • PC(s) con sistema operativo Linux. • Host(s) Virtualizados. • Switch**.** • Router. • Conexión a Internet	1. Identificar herramientas de detección de ataques. 2. Identificar características de modelos de respuesta a incidentes. 3. Comprender los modelos para el manejo de incidentes.	-Estudio de caso -Lista de cotejo.

CIBERSEGURIDAD

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Prácticas de laboratorio -Práctica guiada -Análisis de casos	Analizador de tráfico de red Simulador de redes Software para virtualizar Distribuciones de sistemas operativos abiertos y propietarios Switches Routers Equipo audiovisual Equipo de cómputo Internet

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X	X	

CIBERSEGURIDAD

FUENTES BIBLIOGRÁFICAS

Autor	Año	Título del Documento	Ciudad	País	Editorial
Fundación Telefónica	Año 2016 978-8408163046	*Ciberseguridad. La protección de la información en un mundo digital*	Barcelona	España	Lectura Plus
Nageswara S V Rao , Richard R Brooks , Chase Q Wu	Año 2018 9783319756820	*Proceedings of International Symposium on Sensor Networks, Systems and Security: Advances in Computing and Networking with Applications*	Berlín	Alemania	Springer
Julio Gómez López , Pedro Guillén Núñez, Miguel Ángel De Castro Simón	Año 2014 978-8499645087	*Hackers. Aprende a atacar y defenderte. 2ª edición actualizada*	Madrid	España	RA-MA
Pablo González, Germán Sánchez y Jose Miguel Soriano	Año 2016 978-84-617-9278-8	*Ataques en redes de datos IPv4 e IPv6 3ª*	Madrid	España	0xWord
Carlos García, Valentín Martín y Pablo González	Año 2017 978-84-697-4973-9	*Hacking Windows: Ataques a sistemas y redes Microsoft*	Madrid	España	0xWord