I. Identificación del Curso

Carrera:	Desarrollo de Software			**Modalidad:**	Presencial	**Asignatura UAC:**	Seguridad en infraestructura de tecnologías de información			**Fecha Act:**	Diciembre, 2018
Clave:	18MPEDS0835	**Semestre:**	8	**Créditos:**	5.40	**División:**	Informática y Computación			**Academia:**	Infraestructura de Tecnologías de la información
Horas Total Semana:	3	**Horas Teoría:**	1	**Horas Práctica:**	2	**Horas Semestre:**	54	**Campo Disciplinar:**	Profesional	**Campo de Formación:**	Profesional Extendido

Tabla 1. Identificación de la Planificación del Curso.

II. Adecuación de contenidos para la asignatura

Proposito de la Asignatura (UAC)
Que el estudiante identifique y aplique criterios y políticas de seguridad informática a infraestructuras de tecnologías de información, conociendo los diversos aspectos metodológicos para el control y reforzamiento de la integridad de la información y comunicaciones para lograr que las redes actuales y futuras respondan de manera predecible y consistente con las necesidades de los usuarios.
Competencias Profesionales a Desarrollar (De la carrera)
Evalúa la infraestructura tecnológica sobre la que se integran diferentes servicios, para garantizar la operación y óptimo rendimiento de los equipos de redes informáticas en empresas e instituciones que participan en el mercado laboral.

Tabla 2. Elementos Generales de la Asignatura

III. Competencias de la UAC

Competencias Genéricas.*	
4. Escucha, interpreta y emite mensajes pertinentes en distintos contextos mediante la utilización de medios, códigos y herramientas apropiados. 4.5 Maneja las tecnologías de la información y la comunicación para obtener información y expresar ideas. 8. Participa y colabora de manera efectiva en equipos diversos. 8.2 Aporta puntos de vista con apertura y considera los de otras personas de manera reflexiva.	
Competencias Disciplinares Básicas**	**Competencias Disciplinares Extendidas*****
CO-12 Utiliza las tecnologías de la información y comunicación para investigar, resolver problemas y producir materiales y transmitir información.	COE-10 Analiza los beneficios e inconvenientes del uso de las tecnologías de la información y la comunicación para la optimización de las actividades cotidianas.

Competencias Profesionales Básicas	Competencias Profesionales Extendidas
Evalúa aspectos de seguridad informática e infraestructura de TI aplicando técnicas de control de acceso, filtrado de paquetes, prevención de intrusiones, tráfico de datos, así como criterios y políticas de seguridad para el control y aseguramiento de la integridad de la información que permitan la prevención y recuperación de desastres en redes de cómputo.	- Analiza la evolución de la seguridad informática y los tipos de amenazas, así como los componentes y vulnerabilidades de seguridad aplicando técnicas de mitigación de ataques para comprender los aspectos básicos de la seguridad en redes de cómputo. - Aplica técnicas de control de acceso, filtrado de paquetes y prevención de intrusiones configurando los equipos de red para que proporcionen seguridad a los servicios de red y mitigar el efecto de ataques a la red. - Aplica técnicas para proporcionar seguridad al tráfico de datos transmitido a través de redes públicas usando diversas tecnologías de cifrado y codificación.

Tabla 3. Competencias de la Asignatura.

* Se presentan los atributos de las competencias Genéricas que tienen mayor probabilidad de desarrollarse para contribuir a las competencias profesionales, por lo cual no son limitativas; usted puede seleccionar otros atributos que considere pertinentes. Estos atributos están incluidos en la redacción de las competencias profesionales, por lo que no deben desarrollarse explícitamente o por separado.

** Las competencias Disciplinares no se desarrollarán explícitamente en la UAC. Se presentan como un requerimiento para el desarrollo de las competencias Profesionales.

*** Cada eje curricular debe contener por lo menos una Competencia Disciplinar Extendida.

IV. Habilidades Socioemocionales a desarrollar en la UAC*8

Dimensión	Habilidad
No contiene	No contiene

Tabla 4. Habilidades Construye T

*Estas habilidades se desarrollarán de acuerdo al plan de trabajo determinado por cada plantel. Ver anexo I.

V. Aprendizajes Clave

Eje Disciplinar	Componente	Contenido Central
Desarrollo de Tecnología de la Información.	Infraestructura de TI. Sistemas Operativos y servicios. Seguridad de TI	1. Evolución y evaluación de aspectos de seguridad informática en infraestructura de TI. 2. Configuración de seguridad en dispositivos de red aplicando técnicas de control de acceso, filtrado de paquetes y prevención de intrusiones mediante criterios y políticas de seguridad. 3. Técnicas de seguridad al tráfico de datos a través de redes públicas empleando tecnologías de cifrado y codificación.

VI. Contenidos Centrales de la UAC

Contenido Central	Contenidos Específicos	Aprendizajes Esperados	Proceso de Aprendizaje	Productos Esperados
1. Evolución y evaluación de aspectos de seguridad informática en infraestructura de TI.	- Evolución de la seguridad informática. ¿Cuál es la evolución de la seguridad de la red? ¿Cuáles son los aspectos básicos de la seguridad de la red? ¿Cuáles son las organizaciones internacionales de seguridad? ¿Cuáles son los ámbitos y políticas de seguridad? ¿De qué tipos pueden ser los intrusos en una red? - Amenazas a la red y métodos de ataques informáticos. ¿Cuál es el malware primario? ¿Cuáles son las técnicas de solución de amenazas? ¿Cómo se hace la búsqueda de vulnerabilidades en la red? ¿En qué consisten los intentos de acceso? ¿En qué consisten los ataques de denegación de servicio? ¿Cuáles son las técnicas de solución de ataques? ¿Cuáles son los tipos de ataques capa 2? - Seguridad de punto final. ¿Cuáles son los conceptos de seguridad de acceso y control de malware? ¿Cuáles son los mecanismos de control de acceso a la red y a equipos finales? ¿En qué consisten las auditorias			

informáticas? - Desarrollo de políticas de seguridad. ¿Cuáles son las características y estructura de las políticas de seguridad? ¿Cuáles son las normas, lineamientos y procedimientos, estándares internacionales de seguridad informática? ¿Cuáles son los roles, responsabilidad y conciencia para la seguridad? ¿En qué consiste la capacitación, leyes y ética personal? ¿Cómo será la respuesta a incidentes? ¿En que afecta el factor humano en la seguridad informática y falta de seguridad? - Ciclo de vida del sistema. ¿Cómo es la planeación de continuidad operativa? ¿Cómo es el proceso de recuperación de desastres?	- Reconoce los términos generales de la evolución de la seguridad informática. - Reconoce los términos generales de las amenazas a la red y métodos de ataques informáticos. - Estructura la configuración básica de la seguridad de punto final. - Describe el proceso para establecer una estructura de las políticas de seguridad, normas, lineamientos y procedimientos. - Describe el proceso del ciclo de vida de los sistemas de TI y donde aplica la seguridad.	- Realiza un resumen para distinguir los conceptos generales de las amenazas a la red y métodos de ataques informáticos. - En equipo realiza un cuadro sinóptico utilizando medios audiovisuales para distinguir las estructuras de seguridad de punto final. - Realiza un reporte de caso de estudio empleando el proceso de aseguramiento de seguridad para establecer una estructura de las políticas de seguridad, normas, lineamientos y procedimientos.	- Resumen de los conceptos generales de la evolución de la seguridad informática. - Cuadro sinóptico sobre las amenazas a la red y métodos de ataques informáticos. En equipo. - Reporte de barridos de ping, escaneo de puertos y sniffer de paquetes. En equipo. - Reporte de investigación sobre ataques de redes y herramientas de auditoría. En equipo. - Reporte de caso de estudio para establecer procedimientos, políticas de seguridad, normas y lineamientos.

2. Configuración de seguridad en dispositivos de red aplicando técnicas de control de acceso, filtrado de paquetes y prevención de intrusiones mediante criterios y políticas de seguridad.	- Inspección y administración de equipos de red. ¿Cuáles son los privilegios y roles de acceso? ¿Cómo es el proceso de respaldo del sistema operativo y archivo de configuración? ¿Cómo se emplea el sistema de monitoreo para la seguridad informática? ¿Cómo se usan los protocolos SNMP y NTP para la monitorear la seguridad informática? ¿Cómo es el proceso de acceso a un equipo de red mediante CLI o Telnet? ¿Cuál es el propósito de la centralización de AAA? ¿Cómo es la autentificación local? ¿Para qué sirve un Servidor AAA? ¿Para qué sirve la implementación de AAA con radius? ¿Cuáles son las características y protocolos de comunicación de acceso seguro? ¿Cuáles son los protocolos para sistemas de control de acceso (ACS)? - Implementación de tecnologías firewall. ¿Cuántos tipos de firewall existen? ¿Cómo es el control de acceso basado en contextos? ¿Cuáles son las políticas de firewall basados en zonas? - Implementación de prevención de			

intrusos. ¿En qué consisten las tecnologías de detección de intrusos (IDS) y prevención de intrusiones (IPS)? ¿En qué consisten las tecnologías de prevención de intrusos usando firmas? ¿En qué consiste la implementación de sistemas de prevención de intrusiones? - Técnicas de seguridad para la capa 2. ¿En qué consiste la configuración de restricciones en puertos para equipos activos? ¿Cómo puede darse la reducción de vulnerabilidades en protocolos de control lógico de la red? ¿En qué consiste el control de tráfico excesivo? ¿Cómo se lleva a cabo el monitoreo de puertos usando duplicación de tráfico (Port Mirroring)? ¿En qué consiste la seguridad inalámbrica? - Sistemas criptográficos. ¿En qué consiste la criptografía, criptoanálisis y criptología? ¿En qué consiste la integridad y autenticidad básicas? ¿En qué consisten los algoritmos Hash MD5, SHA-n y HMAC? ¿Cuáles son las técnicas de cifrado (Encryption)? ¿En qué consisten los algoritmos de cifrado (DES, 3DES, AES y otros)? ¿En qué consiste el intercambio de claves Diffie-Hellman?	- Describe los comandos empleados en la configuración básica de privilegios y roles de acceso. - Programa enrutadores para configurar autenticación usando simulador de red y equipo real. - Programa enrutadores para su configuración como firewall empleando listas de acceso usando simulador de red y equipo real. - Programa enrutadores para su configuración en la implementación de prevención de intrusos usando simulador de red y equipo real. - Programa switches para su configuración con técnicas de seguridad para la capa 2 usando simulador de red y equipo real - Describe la criptografía, criptoanálisis y criptología aplicada a la seguridad.	- Realiza un cuadro SQA para distinguir los comandos empleados en la configuración AAA de un enrutador. - En equipo realiza un cuestionario para identificar los comandos empleados en la configuración de un enrutador como firewall empleando listas de acceso. - En equipo realiza una investigación para distinguir los comandos empleados en la configuración para la implementación de prevención de intrusos de un enrutador. - Realiza un resumen para identificar el procedimiento de aseguramiento de seguridad en capa 2 para switches configurables.	- Cuadro SQA sobre el tema de seguridad en dispositivos de red. - Cuestionario sobre los comandos empleados en la configuración AAA de un enrutador. En equipo. - Cuestionario sobre los comandos empleados en la configuración de un enrutador como firewall empleando listas de acceso. En equipo. - Cuestionario sobre los comandos empleados en la configuración para la implementación de prevención de intrusos de un enrutador. En equipo. - Resumen sobre el procedimiento de aseguramiento de seguridad en capa 2 para switches configurables. - Práctica donde implemente un servidor AAA que controle clientes y usuarios que se conectan a los dispositivos de red incluyendo Access Point. En equipo. - Resumen de las técnicas y métodos de cifrado de datos (criptografía, criptoanálisis y criptología).

3. Técnicas de seguridad al tráfico de datos a través de redes públicas empleando tecnologías de cifrado y codificación.	- Reforzamiento de la seguridad en dispositivos de red. ¿Cómo es el acceso a enrutadores de frontera? ¿Cómo es la configuración del sistema de seguridad de acceso? ¿En qué consiste la configuración avanzada de seguridad para conexiones remotas? ¿Cómo es la configuración de comunicación codificada (SSH)? - Redes VPN. ¿Cómo funciona una red VPN? ¿Cuáles son los tipos de redes VPN? ¿En qué consiste una VPN usando Ipsec? ¿En qué consisten las redes VPN de sitio a sitio? ¿En qué consisten las redes VPN de acceso remoto? ¿En qué consisten los túneles SSH? - Planeación y administración de redes seguras. ¿Cuáles son los principios de diseño de redes seguras? ¿En qué consiste la total integración y redes autodefensivas? ¿En qué consiste la operación de la red y pruebas de seguridad?	- Programa enrutadores para configurar la implementación del sistema de seguridad de acceso usando simulador de red y equipo real. - Programa enrutadores para configurarlos en la implementación de redes VPN usando simulador de red y equipo real. - Configura túneles SSH para manipulación de equipos o redireccionamiento de puertos.	- En equipo realiza un cuestionario para distinguir los comandos empleados en la implementación de sistemas de seguridad de acceso de un enrutador. - En equipo realiza una práctica para identificar los comandos empleados en enrutadores para la implementación de redes VPN. - En equipo realiza una práctica para programar un túnel para controlar remotamente equipos o acceder a contenidos inalcanzables en redes normales.	- Cuestionario sobre los comandos empleados en la implementación de sistemas de seguridad de acceso de un enrutador. En equipo. - Cuestionario sobre los comandos empleados en enrutadores para la implementación de redes VPN. En equipo. - Práctica donde configure una red VPN de tal manera que utilice un cliente para conectarse a su servidor VPN. En equipo. - Práctica donde programe un túnel y conexiones o redirecciones de puertos. En equipo.

VII. Recursos bibliográficos, hemerográficos y otras fuentes de consulta de la UAC

Recursos Básicos:
- Cano, J. (2016). Inseguridad de la información - una visión estratégica. México: Alfaomega, Ra-Ma. - Gómez, A. (2016). Enciclopedia de la seguridad informática - 2ª ed.. México: Alfaomega, Ra-Ma.
Recursos Complementarios:
- Fuster, A.; Muñoz, J.; Hernández, L.; Martín, A.; Montoya, F. (2016). Criptografía, protección de datos y aplicaciones - guía para estudiantes y profesionales. México: Alfaomega, Ra-Ma

VIII. Perfil profesiográfico del docente para impartir la UAC

Recursos Complementarios:
Área/Disciplina: Informática. Campo Laboral: Servicios. Tipo de docente: Profesional. Formación Académica: Licenciatura ó Ingeniería, en Electrónica, Sistemas Computacionales e Informática y carreras afines. Constancia de participación en los procesos establecidos en la Ley General del Servicio Profesional Docente, COPEEMS, COSDAC u otros.

XI. Fuentes de Consulta

Fuentes de consulta utilizadas*
- Acuerdo Secretariales relativos a la RIEMS.
- Planes de estudio de referencia del componente básico del marco curricular común de la EMS. SEP-SEMS, México 2017.
- Guía para el Registro, Evaluación y Seguimiento de las Competencias Genéricas, Consejo para la Evaluación de la Educación del Tipo Medio Superior, COPEEMS.
- Manual para evaluar planteles que solicitan el ingreso y la promoción al Padrón de Buena Calidad del Sistema Nacional de Educación Media Superior PBC-SINEMS (Versión 4.0).
- Normas Generales de Servicios Escolares para los planteles que integran el PBC. SINEMS
- Perfiles profesiográficos COPEEMS-2017
- SEP Modelo Educativo 2016.
- Programa Construye T

ANEXO II. Vinculación de las competencias con Aprendizajes esperados

Aprendizajes Esperados	Productos Esperados	Competencias Genéricas con Atributos	Competencias Disciplinares	Competencias profesionales
- Reconoce los términos generales de la evolución de la seguridad informática. - Reconoce los términos generales de las amenazas a la red y métodos de ataques informáticos. - Estructura la configuración básica de la seguridad de punto final. - Describe el proceso para establecer una estructura de las políticas de seguridad, normas, lineamientos y procedimientos. - Describe el proceso del ciclo de vida de los sistemas de TI y donde aplica la seguridad.	- Resumen de los conceptos generales de la evolución de la seguridad informática. - Cuadro sinóptico sobre las amenazas a la red y métodos de ataques informáticos. En equipo. - Reporte de barridos de ping, escaneo de puertos y sniffer de paquetes. En equipo. - Reporte de investigación sobre ataques de redes y herramientas de auditoría. En equipo. - Reporte de caso de estudio para establecer procedimientos, políticas de seguridad, normas y lineamientos.	4. Escucha, interpreta y emite mensajes pertinentes en distintos contextos mediante la utilización de medios, códigos y herramientas apropiados. 4.5 Maneja las tecnologías de la información y la comunicación para obtener información y expresar ideas. 8. Participa y colabora de manera efectiva en equipos diversos. 8.2 Aporta puntos de vista con apertura y considera los de otras personas de manera reflexiva	Básica: CO-12 Utiliza las tecnologías de la información y comunicación para investigar, resolver problemas y producir materiales y transmitir información. Extendida: CO-10 Analiza los beneficios e inconvenientes del uso de las tecnologías de la información y la comunicación para la optimización de las actividades cotidianas.	Básica: Evalúa aspectos de seguridad informática e infraestructura de TI aplicando técnicas de control de acceso, filtrado de paquetes, prevención de intrusiones, tráfico de datos, así como criterios y políticas de seguridad para el control y aseguramiento de la integridad de la información que permitan la prevención y recuperación de desastres en redes de cómputo. Extendida: Analiza la evolución de la seguridad informática y los tipos de amenazas, así como los componentes y vulnerabilidades de seguridad aplicando técnicas de mitigación de ataques para comprender los aspectos básicos de la seguridad en redes de cómputo.

- Describe los comandos empleados en la configuración básica de privilegios y roles de acceso. - Programa enrutadores para configurar autenticación usando simulador de red y equipo real. - Programa enrutadores para su configuración como firewall empleado listas de acceso usando simulador de red y equipo real. - Programa enrutadores para su configuración en la implementación de prevención de intrusos usando simulador de red y equipo real. - Programa switches para su configuración con técnicas de seguridad para la capa 2 usando simulador de red y equipo real - Describe la criptografía, criptoanálisis y criptología aplicada a la seguridad.	- Cuadro SQA sobre el tema de seguridad en dispositivos de red. - Cuestionario sobre los comandos empleados en la configuración AAA de un enrutador. En equipo. - Cuestionario sobre los comandos empleados en la configuración de un enrutador como firewall empleando listas de acceso. En equipo. - Cuestionario sobre los comandos empleados en la configuración para la implementación de prevención de intrusos de un enrutador. En equipo. - Resumen sobre el procedimiento de aseguramiento de seguridad en capa 2 para switches configurables. - Práctica donde implemente un servidor AAA que controle clientes y usuarios que se conectan a los dispositivos de red incluyendo Access Point. En equipo. - Resumen de las técnicas y métodos de cifrado de datos (criptografía, criptoanálisis y criptología).	4. Escucha, interpreta y emite mensajes pertinentes en distintos contextos mediante la utilización de medios, códigos y herramientas apropiados. 4.5 Maneja las tecnologías de la información y la comunicación para obtener información y expresar ideas. 8. Participa y colabora de manera efectiva en equipos diversos. 8.2 Aporta puntos de vista con apertura y considera los de otras personas de manera reflexiva	Básica: CO-12 Utiliza las tecnologías de la información y comunicación para investigar, resolver problemas y producir materiales y transmitir información. Extendida: CO-10 Analiza los beneficios e inconvenientes del uso de las tecnologías de la información y la comunicación para la optimización de las actividades cotidianas.	Básica: Evalúa aspectos de seguridad informática e infraestructura de TI aplicando técnicas de control de acceso, filtrado de paquetes, prevención de intrusiones, tráfico de datos, así como criterios y políticas de seguridad para el control y aseguramiento de la integridad de la información que permitan la prevención y recuperación de desastres en redes de cómputo. Extendida: Aplica técnicas de control de acceso, filtrado de paquetes y prevención de intrusiones configurando los equipos de red para que proporcionen seguridad a los servicios de red y mitigar el efecto de ataques a la red.

- Programa enrutadores para configurar la implementación del sistema de seguridad de acceso usando simulador de red y equipo real. - Programa enrutadores para configurarlos en la implementación de redes VPN usando simulador de red y equipo real. - Configura túneles SSH para manipulación de equipos o redireccionamiento de puertos.	- Cuestionario sobre los comandos empleados en la implementación de sistemas de seguridad de acceso de un enrutador. En equipo. - Cuestionario sobre los comandos empleados en enrutadores para la implementación de redes VPN. En equipo. - Práctica donde configure una red VPN de tal manera que utilice un cliente para conectarse a su servidor VPN. En equipo.	4. Escucha, interpreta y emite mensajes pertinentes en distintos contextos mediante la utilización de medios, códigos y herramientas apropiados. 4.5 Maneja las tecnologías de la información y la comunicación para obtener información y expresar ideas. 8. Participa y colabora de manera efectiva en equipos diversos. 8.2 Aporta puntos de vista con apertura y considera los de otras personas de manera reflexiva	Básica: CO-12 Utiliza las tecnologías de la información y comunicación para investigar, resolver problemas y producir materiales y transmitir información. Extendida: CO-10 Analiza los beneficios e inconvenientes del uso de las tecnologías de la información y la comunicación para la optimización de las actividades cotidianas.	Básica: Evalúa aspectos de seguridad informática e infraestructura de TI aplicando técnicas de control de acceso, filtrado de paquetes, prevención de intrusiones, tráfico de datos, así como criterios y políticas de seguridad para el control y aseguramiento de la integridad de la información que permitan la prevención y recuperación de desastres en redes de cómputo. Extendida: Aplica técnicas para proporcionar seguridad al tráfico de datos transmitido a través de redes públicas usando diversas tecnologías de cifrado y codificación.