



Universidad Guadalajara
Centro Universitario del Sur

Programa de Estudio

1. IDENTIFICACIÓN DE LA UNIDAD DE APRENDIZAJE

División

División de Ciencias Exactas, Naturales y Tecnológicas.

Departamento

Ciencias Computacionales e Innovación Tecnológica.

Academia

Academia de Redes y Comunicaciones.

Programa(s) educativo(s)

Ingeniería en Telemática

Denominación de la unidad de aprendizaje:

Seguridad en Redes de Acceso

Clave de la materia:	Horas de teoría:	Horas de práctica:	Carga horaria global:	Valor en créditos:
IG215	27	53	80	8

Tipo de curso:		Nivel en que se ubica:	Prerrequisitos:
C = curso		Técnico Medio	IG197
CL = curso laboratorio		Técnico Superior	
L = laboratorio		Universitario	
P = práctica		Licenciatura	
T = taller		Especialidad	
CT = curso - taller		Maestría	
N = clínica		Doctorado	
M = módulo			
S = seminario			

Área de formación:

Especializante Selectiva.

Perfil docente:

- Licenciatura en Informática, sistemas computacionales o afines.
- Maestría o Doctorado en áreas de computación, redes o afines.
- Experiencia en manejo de sistemas "Cisco IOS".
- Experiencia en manejo de sistemas "GNU/Linux".
- Acreditación por parte de Cisco Networking Academy. Preferentemente en area de seguridad
- Experiencia en el área de docencia o capacitación mínima un año.

Elaborado por:

Actualizado por:

Mtro. Jesús Enrique Ponce Corona

Fecha de elaboración:

Fecha de última
actualización:

Fecha de última
evaluación:

Fecha de aprobación por
Colegio Departamental:

12/ 07 /2023

1. PRESENTACIÓN DE LA UNIDAD DE APRENDIZAJE

El propósito de esta unidad de aprendizaje es implementar una red de datos segura y actualizada, así como la correcta gestión de licencias de software, tomando en cuenta los requerimientos de los usuarios, la seguridad, calidad de servicio y el desempeño de la red misma. Este propósito se relaciona con el perfil de egreso del Ingeniero en Telemática el cual menciona que "Implementa y administra redes para garantizar las telecomunicaciones de manera segura".

2. OBJETIVO GENERAL/COMPETENCIA

Desarrollar habilidades y conocimientos con base a los servicios de red requeridos por los usuarios, dispositivos, la infraestructura existente y adyacente, así como la estructura de los edificios donde se aplicará, implementando soluciones centralizadas en la administración de equipos de acceso seguro a la red.

- Entender las bases tecnológicas en lo que al diseño de infraestructura y políticas de uso se refiere.
- Establecer propuestas de solución para el respaldo de información del usuario y configuración de equipos.
- Diseña espacios seguros donde los equipos tecnológicos sean correctamente monitoreados y se acceda a ellos de forma supervisada
- Implementar soluciones que prevengan o reduzcan el riesgo a la pérdida de información del usuario, causado por un engaño cibernético..
- Evaluar y analizar casos de estudio como referencia de diseños funcionales para observar tanto los aciertos o las áreas de mejora, que le prepararán para realizar los propios.

3. CAMPO DE APLICACIÓN PROFESIONAL DE LOS CONOCIMIENTOS

Aplicar los conocimientos y habilidades en seguridad de acceso a la red para dar solución a proyectos de infraestructura de conexión, gestión de datos y usuarios, políticas de seguridad que una empresa, institución, organismo requiera. Teniendo transparencia y compatibilidad entre protocolos abiertos y propietarios.

4. SABERES:

Prácticos	<ul style="list-style-type: none">• Analiza las características de las redes instaladas e interpreta los resultados para observar las interacciones y efectos posibles con el diseño en desarrollo• Analiza los requerimientos de los usuarios con el fin de desarrollar un diseño de red adecuado• Caracteriza el tráfico de las aplicaciones de usuario e interpreta los resultados para proponer una solución de seguridad.• Realiza un diseño de red bajo políticas y diseños sólidos y seguros, así como su plan de implementación
Teóricos	<ul style="list-style-type: none">• Identifica los parámetros básicos en el acceso a la red.• Observa la relación entre los factores de desempeño de dispositivos y sus efectos que puedan fortalecer o debilitar las medidas de seguridad.• Aprende a desarrollar entrevistas para obtener los requerimientos de usuario
Formativos	<ul style="list-style-type: none">• Fortalecerá la redacción de documentos técnicos• Fortalecerá las habilidades para expresar y defender sus ideas mediante la presentación y defensa de un proyecto de diseño• Fortalecerá las habilidades de comunicación y trabajo en equipo

5. CONTENIDO TEMÁTICO (TEÓRICO-PRÁCTICO)

1.- Seguridad física

- Seguridad en infraestructura de red
- Diseño de centros de datos
- Diseño arquitectónico
- Protección civil

2.- Seguridad de acceso

- Introducción a los protocolo de acceso
- Diseño de protocolos de acceso físico.
- Manejo de consultores y personal de servicio.
- Estudio de la Ingeniería social
- Análisis de Phising
- Capacitación y prevención de los usuarios.

3.- Seguridad de datos

- Importancia en los respaldos de información.
- Tipos y clasificación de respaldos
- Diseño de plan de respaldo.
- Verificación e integridad de los datos
- Monitoreo y rutinas de respaldos.

4.- Gestión de Software y licencias

- Tipos de licencia de software
- Acuerdos EULA y contrato de soporte
- Manejo de versiones
- Inventario de software
- Diseño de plan de actualizaciones de software

5.- Cifrado de información

- Introducción a la encriptación
- Fundamentos de Hashing
- Análisis de algoritmos de cifrado.
- Herramientas de cifrado.
- Verificación e integridad de los datos.

6.- Controles de Acceso

- Introducción a la autenticación de host y usuarios.
- Análisis de protocolos de autenticación.
- Uso de llaves criptográficas de acceso
- Control de acceso a infraestructuras
- Control de acceso a recursos internos.

•

6. ESTRATEGIAS DE ENSEÑANZA-APRENDIZAJE

- Exposiciones por parte del docente
- Ejercicios teórico-práctico en equipo/individual (solución de ejercicios), por parte de los alumnos
- Realización de trabajo en equipo, individual por parte del alumno.

7. EVALUACIÓN DEL APRENDIZAJE

8.1. Evidencias de aprendizaje	8.2. Criterios de desempeño
Ejercicio práctico de diseño de redes con acceso seguro centralizado.	Se requiere el diseño de una red local básica con políticas de seguridad efectivas.
Ejercicio práctico de configuración de redes con acceso inalámbrico centralizado	Se requiere la configuración de una red local básica con políticas aplicadas a dispositivos de seguridad.
Ejercicio práctico de configuración de redes para aplicar medidas de seguridad y encriptación	Se requiere la implementación y prueba de herramientas criptográficas y su efectivo cifrado sobre los datos del usuario.
Propuesta de gestión de software y correcto respaldos de datos	Planear y diseñar un esquema de trabajo donde las licencias de aplicaciones, actualizaciones y respaldos sean aplicadas de manera segura y constante.

8. CALIFICACIÓN

Reportes de lecturas
Actividades de laboratorio.....
Actividades Prácticas.....
Actividad extracurricular.....

9. ACREDITACIÓN

<p>Periodo ordinario. De conformidad con el artículo 20 del Reglamento General de Evaluación y Promoción de Alumnos de la Universidad de Guadalajara, para que el alumno tenga derecho al registro del resultado final de la evaluación en el periodo ordinario, establecido en el calendario escolar aprobado por el Consejo General Universitario, se requiere:</p> <ol style="list-style-type: none"> I. Estar inscrito en el plan de estudios y curso correspondiente, y II. Tener un mínimo de asistencia del 80% a clases y actividades registradas durante el curso. 	<p>Periodo extraordinario. De conformidad con el artículo 27 del Reglamento General de Evaluación y Promoción de Alumnos de la Universidad de Guadalajara, para que el alumno tenga derecho al registro de la calificación en el periodo extraordinario, se requiere:</p> <ol style="list-style-type: none"> I. Estar inscrito en el plan de estudios y curso correspondiente. II. Haber pagado el arancel y presentar el comprobante correspondiente. III. Tener un mínimo de asistencia del 65% a clases y actividades registradas durante el curso. <p>Se exceptúan de este caso las materias de orden práctico que requerirán la repetición del curso (Art. 23 RGEYPA).</p>
--	---

10. BIBLIOGRAFÍA

BIBLIOGRAFÍA BÁSICA

<ol style="list-style-type: none"> 1. Hacking y Seguridad en Internet. Fernando Picouto Ramos (2008). Ed Alfa Omega 2. Seguridad Digital y Hackers. Juan Diego Gutierrez (2005). Ed Anaya 3. Hacking Tecnicas Fundamentales. Jon Erickson (2009). Ed Anaya 4. Seguridad de Redes. Chris McNab (2008). Brandon A. Nordin (2002). Ed McGraw Hill 5. Hackers. Tecnicas y herramientas para defendernos. Juan Andrés Mailló (2021). Ed RaMa
--

BIBLIOGRAFÍA COMPLEMENTARIA

<ol style="list-style-type: none"> 1. Enciclopedia de la Seguridad Informatica. Alvaro Gomez Vieites (2007). Ed RaMa 2. Seguridad Informatica y Cibercrimen. Moreno Perez Arnoldo (2012). Ed Linea Roja

11. RECURSOS COMPLEMENTARIOS (páginas web, mooc's, plataformas, objetos de aprendizaje)

Plataforma educativa Networking Academy (requiere registro). Curso "Introduction to Cibersecurity":
<https://www.netacad.com/>

Plataforma educativa Fortinet Training Institute (requiere registro). Curso : "Information Security Awareness" <https://training.fortinet.com/auth/saml2/selectidp.php>

Plataforma educativa Fortinet Training Institute (requiere registro). Curso : "Evolution to Cibersecurity"
<https://training.fortinet.com/auth/saml2/selectidp.php>

Plataforma educativa Fortinet Training Institute (requiere registro). Curso : "Fortinet Product Awareness"
<https://training.fortinet.com/auth/saml2/selectidp.php>

Firma:

Presidente de Academia

Vo.Bo.

Jefe de Departamento