



**LA FORMACIÓN ES LA CLAVE
DEL ÉXITO**

Guía del Curso

UF2183 Configuración de la Seguridad de las Redes Inalámbricas de Área Local y Metropolitana

Modalidad de realización del curso: [A distancia y Online](#)

Titulación: [Diploma acreditativo con las horas del curso](#)

OBJETIVOS

Este curso se ajusta a lo expuesto en el itinerario de aprendizaje perteneciente a la Unidad Formativa UF2183 Configuración de la seguridad de las redes inalámbricas de área local y metropolitana, incluida en el Módulo Formativo MF1221_3 Planificación y mantenimiento de redes inalámbricas de área local y metropolitanas, regulada en el Real 628/2013, de 2 de agosto, que permita al alumnado adquirir las competencias profesionales necesarias para organizar y gestionar la puesta en servicio y el mantenimiento de redes inalámbricas de área local y metropolitanas, más concretamente sobre la configuración de la seguridad de las redes inalámbricas de área local y metropolitana.

CONTENIDOS

UNIDAD FORMATIVA 1. CONFIGURACIÓN DE LA SEGURIDAD DE LAS REDES INALÁMBRICAS DE ÁREA LOCAL Y METROPOLITANA

UNIDAD DIDÁCTICA 1. LA SEGURIDAD EN LAS REDES INALÁMBRICAS

1. Vulnerabilidades de una red inalámbrica: evaluación y categorización de los riesgos de seguridad inherentes a las redes de datos inalámbricas:

2. - Intrusión de usuarios no autorizados
3. - Suplantación de Usuario
4. - Seguridad e Integridad de la Información
5. Tipos de ataques a las redes WLAN:
6. - Ataques pasivos
7. - Ataques activos
8. - Espionaje
9. - Escuchas
10. - Ataques de descubrimiento de contraseñas
11. - Puntos de acceso no autorizados
12. - Spoofing
13. - Intercepción
14. - Secuestro de sesiones
15. - Denegación de servicio
16. - Ataque de diccionario
17. Clasificación de las tecnologías de seguridad
18. Mecanismos de seguridad elementales en estaciones base y equipos:
19. - Filtrados MAC
20. - Modificación de la Identificación SSID (de puntos de acceso)
21. - Desactivación de la difusión automática
22. Estándares de seguridad

UNIDAD DIDÁCTICA 2. SISTEMAS DE SEGURIDAD PARA REDES INALÁMBRICAS DE DATOS DE ÁREA LOCAL Y METROPOLITANA

1. Técnicas de cifrado: estático y dinámico. Integridad de datos
2. Protocolo WEP (Wired Equivalent privacy):
3. - Componentes , características y funcionamiento
4. - Vulnerabilidades
5. - Tipos de ataques
6. - Alternativas a WEP: WEP2, WEP dinámico, Red Privada Virtual (VPN)
7. Seguridad basada en la autenticación e identificación de usuarios:
8. - Protocolo EAP (Extensible Authentication Protocol)
9. - Especificación 802.1x

10. - Servidores Radius

UNIDAD DIDÁCTICA 3. SUCESORES DE WEP

1. Acceso protegido de fidelidad inalámbrica (WPA):
2. - Características de WPA
3. - Tecnologías incluidas: IEEE 802.1x, EAP, Temporal Key Integrity Protocol (TKIP), MIC (Message Integrity Code)
4. - Mejoras de WPA respecto a WEP
5. - Modos de funcionamiento de WPA
6. Actualización de los sistemas y mecanismos de seguridad:
7. - WPA2 (IEEE802.11i)
8. - La nueva arquitectura para redes wireless: Robust Security Network (RSN)
9. - Fase operacionales 802.11i
10. Comparativa entre mecanismos de seguridad: WEP, WPA, 802.11i

UNIDAD DIDÁCTICA 4. CONFIGURACIÓN DE LA SEGURIDAD DE UNA RED INALÁMBRICA DE ÁREA LOCAL

1. Seguridad en entornos corporativos. Recomendaciones de diseño
2. Herramientas de acceso remoto
3. Configuración del punto de acceso (AP)
4. Configuración del servidor de autenticación (RADIUS)
5. Configuración de las políticas de filtrado (Firewall)
6. Configuración de los clientes inalámbricos
7. Autenticación de equipos y usuarios mediante EAP (Extended Authentication Protocol)
8. Gestión de certificados digitales para la autenticación de clientes/equipos



C/ San Lorenzo 2 - 2
29001 Málaga



Tlf: 952 215 476
Fax: 951 987 941



www.academiaintegral.com.es
E-mail: info@academiaintegral.com.es