DATOS IDENTIFICATIVOS DE LA UNIDAD FORMATIVA

UNIDAD FORMATIVA	CONFIGURACIÓN DE LA SEGURIDAD DE LAS REDES INALÁMBRICAS DE ÁREA LOCAL Y METROPOLITANA.	DURACIÓN	70
		Condicionada	
Código	UF2183		
Familia profesional	INFORMÁTICA Y COMUNICACIONES		
Área Profesional	Comunicaciones		
Certificado de profesionalidad	MANTENIMIENTO DE SEGUNDO NIVEL EN SISTEMAS DE RADIOCOMUNICACIONES	Nivel	3
Módulo formativo	Planificación y mantenimiento de redes inalámbricas de área local y metropolitanas	Duración	210
Resto de unidades formativas que completan el módulo	Planificación de la puesta en servicio de redes inalámbricas de datos de área local y metropolitana	Duración	90
	Supervisión de redes inalámbricas de área local y metropolitana.		50

Apartado A: **REFERENTE DE COMPETENCIA**

Esta unidad formativa se corresponde con la RP2.

Apartado B: **ESPECIFICACIÓN DE LAS CAPACIDADES Y CONTENIDOS**

Capacidades y criterios de evaluación:

C1: Distinguir los mecanismos y sistemas de seguridad de las redes inalámbricas de área local y metropolitana, y configurar la seguridad de la misma, siguiendo especificaciones técnicas y funcionales dadas.

CE1.1 Describir las principales técnicas de cifrado relacionándolas con el nivel de seguridad ofrecido y los condicionantes impuestos por cada caso, teniendo en cuenta los requisitos de seguridad exigidos.

CE1.2 Explicar las distintas soluciones basadas en protocolos de autenticación de usuarios y en estándares de seguridad, describiendo las funcionalidades y requisitos necesarios.

CE1.3 Identificar los niveles y filtros de protección configurables en un punto de acceso inalámbrico en función de las especificaciones técnicas.

CE1.4 Explicar los procedimientos básicos destinados a garantizar la seguridad de los equipos de usuarios asociados a la red inalámbrica.

CE1.5 Realizar la configuración de los parámetros de seguridad de un punto de acceso inalámbrico, según necesidades dadas:

- Determinar los puntos fuertes y los puntos débiles en términos de seguridad.
- Modificar el valor por defecto del identificador SSID y desactivar su difusión automática.
- Establecer reglas de filtrado relacionadas con las direcciones físicas de los equipos asociados.
- Definir claves de cifrado acordes a las técnicas de encriptación y autenticación seleccionadas.
- Configurar en los equipos de usuario los parámetros de seguridad adecuados y comprobar su correcta asociación con el punto de acceso.
- Documentar los procesos realizados siguiendo formatos especificados.
- Interpretar la documentación técnica asociada, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda.

Contenidos:

1. La seguridad en las redes inalámbricas

- Vulnerabilidades de una red inalámbrica: evaluación y categorización de los riesgos de seguridad inherentes a las redes de datos inalámbricas:
  - Intrusión de usuarios no autorizados.
  - Suplantación de Usuario.
  - Seguridad e Integridad de la Información.
- Tipos de ataques a las redes WLAN:

- – Ataques pasivos.
- – Ataques activos.
- – Espionaje.
- – Escuchas.
- – Ataques de descubrimiento de contraseñas.
- – Puntos de acceso no autorizados.
- – Spoofing.
- – Intercepción.
- – Secuestro de sesiones.
- – Denegación de servicio.
- – Ataque de diccionario.
- – Clasificación de las tecnologías de seguridad.
- – Mecanismos de seguridad elementales en estaciones base y equipos:
  - – Filtrados MAC.
  - – Modificación de la Identificación SSID (de puntos de acceso).
  - – Desactivación de la difusión automática.
- – Estándares de seguridad.

2. Sistemas de seguridad para redes inalámbricas de datos de área local y metropolitana

- – Técnicas de cifrado: estático y dinámico. Integridad de datos.
- – Protocolo WEP (Wired Equivalent privacy):
  - – Componentes , características y funcionamiento.
  - – Vulnerabilidades.
  - – Tipos de ataques.
  - – Alternativas a WEP: WEP2, WEP dinámico, Red Privada Virtual (VPN).
- – Seguridad basada en la autentificación e identificación de usuarios:
  - – Protocolo EAP (Extensible Authentication Protocol).
  - – Especificación 802.1x.
- – Servidores Radius.

3. Sucesores de WEP

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

4. Configuración de la seguridad de una red inalámbrica de área local

- – Seguridad en entornos corporativos. Recomendaciones de diseño.
- – Herramientas de acceso remoto.
- – Configuración del punto de acceso (AP).
- – Configuración del servidor de autenticación (RADIUS).
- – Configuración de las políticas de filtrado (Firewall).
- – Configuración de los clientes inalámbricos.
- – Autenticación de equipos y usuarios mediante EAP (Extended Autentication Protocol).
- – Gestión de certificados digitales para la autenticación de clientes/equipos.

Apartado C: **REQUISITOS Y CONDICIONES**

Deberá cumplir alguno de los requisitos siguientes:

- Estar en posesión del título de Bachiller.
- Estar en posesión de algún certificado de profesionalidad de nivel 3.
- Estar en posesión de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional.
- Cumplir el requisito académico de acceso a los ciclos formativos de grado superior o haber superado las correspondientes pruebas de acceso a ciclos de grado superior.

- Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
- Tener, de acuerdo con la normativa que se establezca, los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.

En relación con las exigencias de los formadores o de las formadoras, instalaciones y equipamientos se atenderá las exigencias solicitadas para el propio certificado de profesionalidad.