

# MikroTik

---

Certified Security  
Engineer (MTCSE)

---

# hotelinking

## Certificación

MikroTik MTCSE

## Duración

2 días (16 horas)

## Precio

450 €

Formación Bonificable (solicitar más información: [admin@hotelinking.com](mailto:admin@hotelinking.com))

## Fecha

Del 23 y 24 de marzo de 2023

## Horario del curso:

**Jueves:** de 9 a 18 h. (incluye 1 hora para comer)

**Viernes:** de 9 a 18 h. (incluye 1 hora para comer)

## Lugar

Parc Bit. Palma de Mallorca

## Resultado:

Al final del curso, el/la participante será capaz de planificar e implementar medidas adecuadas de seguridad en las redes que gestione.

## Público al que va dirigido:

Ingenieros y técnicos de redes que quieran desplegar y mantener redes seguras basadas en dispositivos MikroTik.

## Prerrequisitos del curso:

Certificado MTCNA

Título	Objetivo
<b>Módulo 1 Introducción</b>	<ul style="list-style-type: none"> <li>■ Ataques, mecanismos y servicios</li> <li>■ Amenazas más frecuentes</li> <li>■ Implementación de seguridad en RouterOS</li> <li>■ <b>Módulo 1 Laboratorio</b></li> </ul>

Título	Objetivo
<b>Módulo 2 Firewall</b>	<ul style="list-style-type: none"> <li>■ Flujo de paquetes, cadenas del firewall</li> <li>■ Firewall basado en estados</li> <li>■ Tabla RAW</li> <li>■ Mitigar ataques basados en SYN flood usando la tabla RAW</li> <li>■ Configuración por defecto en RouterOS</li> <li>■ Prácticas recomendadas para el acceso de gestión</li> <li>■ Detección de ataques a servicios críticos</li> <li>■ Filtrado en Bridge</li> <li>■ Opciones avanzadas de filtrado en firewall</li> <li>■ Filtrado ICMP</li> <li>■ <b>Módulo 2 Laboratorio</b></li> </ul>

Título	Objetivo
<b>Módulo 3 Ataques en capa OSI</b>	<ul style="list-style-type: none"> <li>■ Ataques MNDP y prevención</li> <li>■ DHCP: servidores intrusos, ataques de agotamiento y prevención</li> <li>■ Ataques TCP SYN y prevención</li> <li>■ Ataques UDP y prevención</li> <li>■ Ataques ICMP Smurf y prevención</li> <li>■ FTP, telnet y SSH: ataques por fuerza bruta y prevención</li> <li>■ Detectar escaneo de puertos y prevención</li> <li>■ <b>Módulo 3 Laboratorio</b></li> </ul>

Título	Objetivo
<b>Módulo 4 Criptografía</b>	<ul style="list-style-type: none"> <li>■ Introducción a la criptografía y terminología</li> <li>■ Métodos de cifrado</li> <li>■ Algoritmos - simétricos, asimétricos</li> <li>■ Infraestructura de claves pública (PKI)</li> <li>■ Certificados <ul style="list-style-type: none"> <li>■ Certificados autofirmados</li> <li>■ Certificados gratuitos válidos</li> <li>■ Utilizando certificados en RouterOS</li> </ul> </li> <li>■ <b>Módulo 4 Laboratorio</b></li> </ul>

Título	Objetivo
<b>Módulo 5 Securizando el router</b>	<ul style="list-style-type: none"> <li>■ Port knocking</li> <li>■ Conexiones seguras (HTTPS, SSH, WinBox)</li> <li>■ Puertos por defecto de servicios</li> <li>■ Túneles a través de SSH</li> <li>■ <b>Módulo 5 Laboratorio</b></li> </ul>

Título	Objetivo
<b>Módulo 6 Túneles seguros</b>	<ul style="list-style-type: none"> <li>■ Introducción a IPsec</li> <li>■ L2TP + IPsec</li> <li>■ SSTP con certificados</li> <li>■ <b>Módulo 6 Laboratorio</b></li> </ul>

# hotelinking

CONTACTLESS TECH TO CONNECT WITH YOUR GUESTS

Carretera de Valldemossa, Km. 7,4 Parc Bit. Edifici Disset 3ª Planta Puerta D7, 07120

[www.hotelinking.com](http://www.hotelinking.com) | [help@hotelinking.com](mailto:help@hotelinking.com)

