



Gracias a



[openwebinars.net/cert/QTEK](https://openwebinars.net/cert/QTEK)



OpenWebinars certifica que

**Fernando Gonzalez Anton**

Ha superado con éxito

**Redes y Seguridad en AWS**

Duración del curso

**10 horas**

Fecha de expedición

**24 febrero 2026**

A handwritten signature in black ink, appearing to read 'Manuel Agudo', positioned over a large, light gray watermark of the OpenWebinars logo.

CEO de OpenWebinars

**Manuel Agudo**

## Contenido

# Redes y Seguridad en AWS

### 1. INTRODUCCIÓN A LAS REDES EN AWS CON AMAZON VPC

Presentación

¿Qué es Amazon VPC y por qué es esencial?

Diseño de una arquitectura de red en VPC

Subnets, tablas de enrutamiento y gateways (Internet Gateway, NAT Gateway)

Grupos de seguridad y NACLs (Network Access Control Lists)

Peering de VPC y conectividad entre regiones

Monitoreo y registro de redes con VPC Flow Logs

Test Autoevaluación

### 2. GESTIÓN DE IDENTIDADES Y ACCESOS CON IAM

¿Qué es IAM y cómo se utiliza en AWS?

Usuarios y grupos en IAM

Políticas de permisos: Principios de privilegio mínimo

Roles de IAM para servicios (EC2, Lambda, etc)

MFA (Autenticación Multifactor) para fortalecer la seguridad

Control de acceso condicional y permisos basados en políticas

Auditoría de seguridad y compliance con IAM Access Analyzer

Test Autoevaluación

### 3. SEGURIDAD DE REDES: AWS SHIELD Y AWS WAF

Introducción a AWS Shield y protección DDoS

Diferencias entre AWS Shield Standard y Advanced

Configuración de AWS WAF para mitigar ataques web

Creación de reglas personalizadas en WAF para protección de aplicaciones

Integración de WAF con servicios como CloudFront y API Gateway



Test Autoevaluación

## **4. CIFRADO Y GESTIÓN DE CLAVES: AWS KEY MANAGEMENT SERVICE (KMS)**

Introducción a AWS KMS: Gestión de claves de cifrado

Crear y gestionar claves de cifrado en KMS

Cifrado en reposo y en tránsito con KMS

Uso de la clave para cifrar y descifrar

Rotación automática de claves y auditoría de uso de KMS

Caso de uso: Cifrado de datos sensibles con KMS

Test Autoevaluación

## **5. OTRAS SOLUCIONES DE SEGURIDAD AVANZADA EN AWS**

Protección avanzada con Amazon GuardDuty (detección de amenazas)

AWS Macie: Identificación de datos sensibles y PII en S3

AWS Secrets Manager: Gestión segura de secretos y credenciales

AWS Inspector: Evaluación automatizada de vulnerabilidades en instancias EC2

Test Autoevaluación

## **6. CASOS DE USO PRÁCTICOS Y PROYECTOS**

Caso de uso I: Encontrar vulnerabilidades con Amazon Inspector

Caso de uso II: Detección de datos sensibles con Amazon Macie

Caso de uso III: Monitorear el cifrado con CloudTrail

Caso de uso IV: Revisar los grupos de seguridad con AWS Config

## **7. CONCLUSIONES**

Conclusiones y próximos pasos