



Curso Security Engineering on AWS



Calle de la Basílica, 19
28020 Madrid
(34) 915 53 61 62
www.cas-training.com





AWS-SEA

CAS Training

**Nivel**

Intermedio

**Duración**

21 horas

**Modalidad**

Aula Virtual

**Learning
by doing****Curso
Oficial**

Curso Security Engineering on AWS

Dirigido a:

- Ingenieros de seguridad.
- Arquitectos de seguridad.
- Arquitectos de la nube.
- Operadores de la nube.

Objetivos:

- Exponer una comprensión de la seguridad en la nube de AWS basada en la tríada de la CIA.
- Crear y analizar la autenticación y las autorizaciones con IAM.
- Administrar y aprovisionar cuentas en AWS con los servicios de AWS adecuados.
- Identificar cómo administrar los secretos mediante los servicios de AWS.
- Supervisar la información confidencial y proteger los datos mediante el cifrado y los controles de acceso.
- Identificar los servicios de AWS que abordan los ataques de fuentes externas.
- Supervisar, generar y recopilar registros.
- Identificar indicadores de incidentes de seguridad.
- Identificar cómo investigar las amenazas y mitigarlas con los servicios de AWS.

Requisitos:

- Haber completado, previamente, los cursos AWS Security Essentials y Architecting on AWS.
- Tener conocimientos prácticos sobre prácticas de seguridad y conceptos de la infraestructura de TI.
- Estar familiarizado con la nube de AWS.

Material del curso:

Documentación oficial del **curso Security Engineering on AWS**.

Perfil del docente:

- Formador certificado por AWS.
- Más de 5 años de experiencia profesional.
- Más de 4 años de experiencia docente.
- Profesional activo en empresas del sector IT.

Metodología:

- “Learning by doing” se centra en un contexto real y concreto, buscando un aprendizaje en equipo para la resolución de problemas en el sector empresarial.
- Aulas con grupos reducidos para que el profesional adquiera la mejor atención por parte de nuestros instructores profesionales.
- El programa de estudios como partners oficiales es confeccionado por nuestro equipo de formación y revisado por las marcas de referencia en el sector.
- La impartición de las clases podrá ser realizada tanto en modalidad Presencial como Virtual.





Examen y Certificación:

Preparación para el examen de certificación: AWS Certified Security Specialty





Contenidos:

Módulo 1: Security Overview and Review

- Explain Security in the AWS Cloud.
- Explain AWS Shared Responsibility Model.
- Summarize IAM, Data Protection, and Threat Detection and Response.
- State the different ways to interact with AWS using the console, CLI, and SDKs.
- Describe how to use MFA for extra protection.
- State how to protect the root user account and access keys.

Módulo 2: Securing Entry Points on AWS

- Describe how to use multi-factor authentication (MFA) for extra protection.
- Describe how to protect the root user account and access keys.
- Describe IAM policies, roles, policy components, and permission boundaries.
- Explain how API requests can be logged and viewed using AWS CloudTrail and how to view and analyze access history.
- Hands-On Lab: Using Identity and Resource Based Policies.

Módulo 3: Account Management and Provisioning on AWS

- Explain how to manage multiple AWS accounts using AWS Organizations and AWS Control Tower.
- Explain how to implement multi-account environments with AWS Control Tower.
- Demonstrate the ability to use identity providers and brokers to acquire access to AWS services.
- Explain the use of AWS IAM Identity Center (successor to AWS Single Sign-On) and AWS Directory Service.
- Demonstrate the ability to manage domain user access with Directory Service and IAM Identity Center.
- Hands-On Lab: Managing Domain User Access with AWS Directory Service

Módulo 4: Secrets Management on AWS

- Describe and list the features of AWS KMS, CloudHSM, AWS Certificate Manager (ACM), and AWS Secrets Manager.
- Demonstrate how to create a multi-Region AWS KMS key.
- Demonstrate how to encrypt a Secrets Manager secret with an AWS KMS key.
- Demonstrate how to use an encrypted secret to connect to an Amazon Relational Database Service (Amazon RDS) database in multiple AWS Regions
- Hands-on lab: Lab 3: Using AWS KMS to Encrypt Secrets in Secrets Manager

Módulo 5: Data Security

- Monitor data for sensitive information with Amazon Macie.
- Describe how to protect data at rest through encryption and access controls.
- Identify AWS services used to replicate data for protection.
- Determine how to protect data after it has been archived.
- Hands-on lab: Lab 4: Data Security in Amazon S3

Módulo 6: Infrastructure Edge Protection

- Describe the AWS features used to build secure infrastructure.
- Describe the AWS services used to create resiliency during an attack.
- Identify the AWS services used to protect workloads from external threats.
- Compare the features of AWS Shield and AWS Shield Advanced.
- Explain how centralized deployment for AWS Firewall Manager can enhance security.
- Hands-on lab: Lab 5: Using AWS WAF to Mitigate Malicious Traffic

Módulo 7: Monitoring and Collecting Logs on AWS

- Identify the value of generating and collecting logs.
- Use Amazon Virtual Private Cloud (Amazon VPC) Flow Logs to monitor for security events.
- Explain how to monitor for baseline deviations.
- Describe Amazon EventBridge events.
- Describe Amazon CloudWatch metrics and alarms.
- List log analysis options and available techniques.
- Identify use cases for using virtual private cloud (VPC) Traffic Mirroring.
- Hands-on lab: Lab 6: Monitoring for and Responding to Security Incidents

Módulo 8: Responding to Threats

- Classify incident types in incident response.





- Understand incident response workflows.
- Discover sources of information for incident response using AWS services.
- Understand how to prepare for incidents.
- Detect threats using AWS services.
- Analyze and respond to security findings.
- Hands-on lab: Lab 7: Incident Response





CAS TRAINING

UN ESPACIO PARA CRECER

cas-training.com

Curso Security Engineering on AWS
AWS-SEA

Microsoft
Partner



ORACLE

Partner

ORACLE
University

Digital Distribution Partner

OPENEDG
Channel
Partner

