
Security in Google Cloud

Duración: 3 Días **Código del Curso: GO5977** **Version: 2.1.1** **Método de Impartición: Curso Remoto (Virtual)**

Temario:

This course gives participants broad study of security controls and techniques on Google Cloud. Through lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure GCP solution. Participants also learn mitigation techniques for attacks at many points in a GCP-based infrastructure, including Distributed Denial-of-Service attacks, phishing attacks, and threats involving content classification and use.

Curso Remoto (Abierto)

Nuestra solución de formación remota o virtual, combina tecnologías de alta calidad y la experiencia de nuestros formadores, contenidos, ejercicios e interacción entre compañeros que estén atendiendo la formación, para garantizar una sesión formativa superior, independiente de la ubicación de los alumnos.

Dirigido a:

This class is intended for the following job roles:

- ? Cloud information security analysts, architects, and engineers
 - ? Information security/cybersecurity specialists
 - ? Cloud infrastructure architects
 - ? Developers of cloud applications
-

Objetivos:

- | | |
|--|---|
| ■ This course teaches participants the following skills: | ■ ? Implementing Identity Aware Proxy |
| ■ ? Understanding the Google approach to security | ■ ? Analyzing changes to the configuration or metadata of resources with GCP audit logs |
| ■ ? Managing administrative identities using Cloud Identity. | ■ ? Scanning for and redact sensitive data with the Data Loss Prevention API |
| ■ ? Implementing least privilege administrative access using Google Cloud Resource | ■ ? Scanning a GCP deployment with Forseti |
| ■ Manager, Cloud IAM. | ■ ? Remediating important types of vulnerabilities, especially in public access to data and |
| ■ ? Implementing IP traffic controls using VPC firewalls and Cloud Armor | ■ VMs |
-

Prerequisites:

To get the most out of this course, participants should have:

? Prior completion of Google Cloud Platform Fundamentals: Core Infrastructure or

equivalent experience

? Prior completion of Networking in Google Cloud Platform or equivalent experience

? Knowledge of foundational concepts in information security:

? Fundamental concepts:

| vulnerability, threat, attack surface

| confidentiality, integrity, availability

Common threat types and their mitigation

strategies

? Public-key cryptography

| Public and private key pairs

| Certificates

| Cipher types

| Key width

? Certificate authorities

? Transport Layer Security/Secure Sockets Layer encrypted communication

? Public key infrastructures

? Security policy

? Basic proficiency with command-line tools and Linux operating system environments

? Systems Operations experience, including deploying and managing applications, either

on-premises or in a public cloud environment

? Reading comprehension of code in Python or JavaScript

Contenido:

Module 1	Module 5	? Cloud Security Scanner
Foundations of GCP	Securing Compute Engine:	? Lab: Using Cloud Security Scanner to find vulnerabilities in an App
Security	techniques and best	Engine application
? Understand the GCP shared security responsibility model	practices	? Identity Aware Proxy
? Understand Google Cloud's approach to security	? Compute Engine service accounts, default and customer-defined	? Lab: Configuring Identity Aware Proxy to protect a project
? Understand the kinds of threats mitigated by Google and by GCP	? IAM roles for VMs	Module 8
? Define and Understand Access Transparency and Access Approval	? API scopes for VMs	Securing Kubernetes:
(beta)	? Managing SSH keys for Linux VMs	techniques and best
Module 2	? Managing RDP logins for Windows VMs	practices
Cloud Identity	? Organization policy controls: trusted images, public IP address,	? Authorization
? Cloud Identity	disabling serial port	? Securing Workloads
? Syncing with Microsoft Active Directory using Google Cloud Directory	? Encrypting VM images with customer-managed encryption keys and	? Securing Clusters
Sync	with customer-supplied encryption keys	? Logging and Monitoring
? Using Managed Service for Microsoft Active Directory (beta)	? Finding and remediating public access to VMs	PART III: MITIGATING VULNERABILITIES IN GOOGLE CLOUD
? Choosing between Google authentication and SAML-based SSO	? Best practices, including using hardened custom images, custom	Module 9
? Best practices, including DNS configuration, super admin accounts	service accounts (not the default service account), tailored API	Protecting against
? Lab: Defining Users with Cloud Identity Console	scopes, and the use of application default credentials instead of	Distributed Denial of Service
Module 3	user-managed keys	Attacks
	? Lab: Configuring, using, and auditing VM service accounts and scopes	? How DDoS attacks work
		? Mitigations: GCLB, Cloud CDN, autoscaling, VPC ingress and egress

Identity, Access, and Key		firewalls, Cloud Armor (including its rules language)
Management	? Encrypting VM disks with customer-supplied encryption keys	
? GCP Resource Manager: projects, folders, and organizations	? Lab: Encrypting disks with customer-supplied encryption keys	? Types of complementary partner products
? GCP IAM roles, including custom roles	? Using Shielded VMs to maintain the integrity of virtual machines	? Lab: Configuring GCLB, CDN, traffic blacklisting with Cloud Armor
? GCP IAM policies, including organization policies	Module 6	Module 10
? GCP IAM Labels	Securing cloud data:	Protecting against
? GCP IAM Recommender	techniques and best	content-related
? GCP IAM Troubleshooter	practices	vulnerabilities
? GCP IAM Audit Logs	? Cloud Storage and IAM permissions	? Threat: Ransomware
? Best practices, including separation of duties and least privilege, the	? Cloud Storage and ACLs	? Mitigations: Backups, IAM, Data Loss Prevention API
use of Google groups in policies, and avoiding the use of primitive	? Auditing cloud data, including finding and remediating publicly	? Threats: Data misuse, privacy violations, sensitive/restricted/unacceptable content
roles	accessible data	? Threat: Identity and OAuth phishing
? Labs: Configuring Cloud IAM, including custom roles and organization	? Signed Cloud Storage URLs	? Mitigations: Classifying content using Cloud ML APIs; scanning and
policies	? Signed policy documents	redacting data using Data Loss Prevention API
Module 4	? Encrypting Cloud Storage objects with customer-managed encryption	? Lab: Redacting Sensitive Data with Data Loss Prevention API
Configuring Google Virtual	keys and with customer-supplied encryption keys	Module 11
Private Cloud for Isolation	? Best practices, including deleting archived versions of objects after	Monitoring, Logging,
and Security	key rotation	Auditing, and Scanning
? Configuring VPC firewalls (both ingress and egress rules)	? Lab: Using customer-supplied encryption keys with Cloud Storage	? Security Command Center
? Load balancing and SSL policies	? Lab: Using customer-managed encryption	? Stackdriver monitoring and logging

? Private Google API access	keys with Cloud Storage	? Lab: Installing Stackdriver agents
? SSL proxy use	and Cloud KMS	
? Best practices for VPC networks, including peering and shared VPC	? BigQuery authorized views	? Lab: Configuring and using Stackdriver monitoring and logging
use, correct use of subnetworks	? BigQuery IAM roles	? VPC flow logs
? Best security practices for VPNs	? Best practices, including preferring IAM permissions over ACLs	? Lab: Viewing and using VPC flow logs in Stackdriver
? Security considerations for interconnect and peering options	? Lab: Creating a BigQuery authorized view	? Cloud audit logging
? Available security products from partners	Module 7	? Lab: Configuring and viewing audit logs in Stackdriver
? Defining a service perimeter, including perimeter bridges	Securing Applications:	? Deploying and Using Forseti
? Setting up private connectivity to Google APIs and services	techniques and best practices	? Lab: Inventorying a Deployment with Forseti Inventory (demo)
? Lab: Configuring VPC firewalls	? Types of application security vulnerabilities	? Lab: Scanning a Deployment with Forseti Scanner (demo)
PART II: SECURITY BEST PRACTICES ON GOOGLE CLOUD	? DoS protections in App Engine and Cloud Functions	

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid