INEFOP

INEFOP en Coursera: Programa 2: Certificaciones Profesionales de Google - Seguridad					
Nombre del curso	**Descripcion del curso**	**Idioma del curso**	**Cursos con subtitulos**	**Institución**	**Nivel de dificultad**
Google Cloud Platform Fundamentals: Core Infrastructure	This course introduces you to important concepts and terminology for working with Google Cloud Platform (GCP). You learn about, and compare, many of the computing and storage services available in Google Cloud Platform, including Google App Engine, Google Compute Engine, Google Kubernetes Engine, Google Cloud Storage, Google Cloud SQL, and BigQuery. You learn about important resource and policy management tools, such as the Google Cloud Resource Manager hierarchy and Google Cloud Identity and Access Management. Hands-on labs give you foundational skills for working with GCP.\n\nNote:\n•Google services are currently unavailable in China.	Inglés	SI	Google Cloud	Principiante
Hands-On Labs in Google Cloud for Security Engineers	Security is an uncompromising feature of Google Cloud services, and Google Cloud has developed specific tools for ensuring safety and identity across your projects. In this course you will get added hands-on practice understanding and securing resources with multiple Google Cloud services including Google Kubernetes Engine (GKE).\n \nThis course is unlike other courses, in that it consists of one module of background videos, followed by a series of hands-on practice exercises on Google Cloud via Qwiklabs. The practice modules include no videos, lectures, or quizzes - just more practice on real Google Cloud.\n\nIf you enjoyed this course, you can check out the full quest including a challenge lab that requires a solution to be built with minimal guidance. You will have an opportunity to earn a Google Cloud digital Skill Badge on completion as well! Visit - google.qwiklabs.com and look for ‘Secure Workloads in Google Kubernetes Engine’ and ‘Ensure Access & Identity in Google Cloud’.	Inglés	SI	Google Cloud	Principiante
Networking in Google Cloud: Defining and Implementing Networks	This course gives participants a broad study of networking options on\n Google Cloud. Through recorded lectures, demonstrations, and hands-on labs, participants\n explore and deploy Google Cloud networking technologies, such as Google Virtual\n Private Cloud (VPC) networks, subnets and firewalls. The course also covers access\n control to networks, sharing networks and load balancing.	Inglés	NO	Google Cloud	Principiante
Networking in Google Cloud: Hybrid Connectivity and Network Management	This course builds on the Networking in Google Cloud: Defining and Implementing\n Networks course and enhances participants study of networking options on Google\n Cloud. Through recorded lectures, demonstrations, and hands-on labs, participants\n explore and deploy Google Cloud networking technologies, such as the interconnection\n among networks, common network design patterns and the automated deployment of networks\n using Deployment Manager or Terraform. The course also covers networking pricing\n and billing to help you optimize your network spend and monitoring and logging\n features that can help you troubleshoot your Google Cloud network infrastructure.	Inglés	NO	Google Cloud	Principiante

Managing Security in Google Cloud Platform	This self-paced training course gives participants broad study of security controls and techniques on Google Cloud Platform.\n\nThrough recorded lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure GCP solution, including Cloud Identity, the GCP Resource Manager, Cloud IAM, Google Virtual Private Cloud firewalls, Google Cloud Load balancing, Cloud CDN, Cloud Storage access control technologies, Stackdriver, Security Keys, Customer-Supplied Encryption Keys, the Google Data Loss Prevention API, and Cloud Armor. Participants learn mitigations 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.\n\nTo get the most out of this course, participants should have:\n * Prior completion of Google Cloud Platform Fundamentals: Core Infrastructure or equivalent experience\n * Prior completion of GCP and Hybrid Networking Deep Dive or equivalent experience\n * Knowledge of foundational concepts in information security, such as\n * vulnerability, threat, attack surface \n * confidentiality, integrity, availability\n * common threat types and their mitigation strategies\n * public-key cryptography\n * public and private key pairs\n * certificates\n * cipher types\n * certificate authorities\n * Transport Layer Security/Secure Sockets Layer encrypted communication\n * public key infrastructures\n * security policy\n * Basic proficiency with command-line tools and Linux operating system environments\n * Systems Operations experience, deploying and managing applications, on-premises or in a public cloud environment\n * Reading comprehension of code in Python or Javascript\n\n>>> By enrolling in this course you agree to the Qwiklabs Terms of Service as set out in the FAQ and located at: https://qwiklabs.com/terms_of_service <<<	Inglés	NO	Google Cloud	Principiante
Security Best Practices in Google Cloud	This self-paced training course gives participants broad study of security controls and techniques on Google Cloud Platform.\n\nThrough recorded lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure GCP solution, including Cloud Identity, the GCP Resource Manager, Cloud IAM, Google Virtual Private Cloud firewalls, Google Cloud Load balancing, Cloud CDN, Cloud Storage access control technologies, Stackdriver, Security Keys, Customer-Supplied Encryption Keys, Security Command Center, the Google Data Loss Prevention API, and Cloud Armor. Participants learn mitigations 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.\n\nTo get the most out of this course, participants should have:\n * Prior completion of Google Cloud Platform Fundamentals: Core Infrastructure or equivalent experience\n * Prior completion of GCP and Hybrid Networking Deep Dive or equivalent experience\n * Knowledge of foundational concepts in information security, such as\n * vulnerability, threat, attack surface \n * confidentiality, integrity, availability\n * common threat types and their mitigation strategies\n * public-key cryptography\n * public and private key pairs\n * certificates\n * cipher types\n * certificate authorities\n * Transport Layer Security/Secure Sockets Layer encrypted communication\n * public key infrastructures\n * security policy\n * Basic proficiency with command-line tools and Linux operating system environments\n * Systems Operations experience, deploying and managing applications, on-premises or in a public cloud environment\n * Reading comprehension of code in Python or Javascript\n\n>>> By enrolling in this course you agree to the Qwiklabs Terms of Service as set out in the FAQ and located at: https://qwiklabs.com/terms_of_service <<<	Inglés	NO	Google Cloud	Principiante
Mitigating Security Vulnerabilities on Google Cloud Platform	This self-paced training course gives participants broad study of security controls and techniques on Google Cloud Platform.\n\nThrough recorded lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure GCP solution, including Cloud Identity, the GCP Resource Manager, Cloud IAM, Google Virtual Private Cloud firewalls, Google Cloud Load balancing, Cloud CDN, Cloud Storage access control technologies, Stackdriver, Security Keys, Customer-Supplied Encryption Keys, the Google Data Loss Prevention API, and Cloud Armor. Participants learn mitigations 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.\n\nTo get the most out of this course, participants should have:\n * Prior completion of Google Cloud Platform Fundamentals: Core Infrastructure or equivalent experience\n * Prior completion of GCP and Hybrid Networking Deep Dive or equivalent experience\n * Knowledge of foundational concepts in information security, such as\n * vulnerability, threat, attack surface \n * confidentiality, integrity, availability\n * common threat types and their mitigation strategies\n * public-key cryptography\n * public and private key pairs\n * certificates\n * cipher types\n * certificate authorities\n * Transport Layer Security/Secure Sockets Layer encrypted communication\n * public key infrastructures\n * security policy\n * Basic proficiency with command-line tools and Linux operating system environments\n * Systems Operations experience, deploying and managing applications, on-premises or in a public cloud environment\n * Reading comprehension of code in Python or Javascript\n\n>>> By enrolling in this course you agree to the Qwiklabs Terms of Service as set out in the FAQ and located at: https://qwiklabs.com/terms_of_service <<<	Inglés	NO	Google Cloud	Principiante