PROFESSIONAL CLOUD SECURITY ENGINEER · CHEAT SHEET · CERTIFYDECK

Google Cloud Certified Professional Cloud Security Engineer

Dominios, pesos oficiales y habilidades clave del temario de Professional Cloud Security Engineer, para repasar antes del examen.

Nivel: Advanced (Professional) Duración: 120 min Fuente: guía de estudio oficial de Microsoft Learn

1. Configuring access

25–25%

Managing Cloud Identity

- Configuring Google Cloud Directory Sync and implement single sign-on (SSO) with a third-party identity provider
- Managing a super administrator account
- El IdP externo o el sistema de RR. HH. debe ser la fuente de verdad: los cambios se hacen allí y el aprovisionamiento automático (GCDS, conectores de Entra ID u Okta) los propaga a Cloud Identity. Propaga también suspensiones y eliminaciones; suspender en Cloud Identity cierra sesiones e invalida tokens, y las cuentas huérfanas permiten reutilizar nombres. Mantén las identidades de Cloud Identity como subconjunto de las del IdP.
- La Admin SDK Directory API crea, actualiza, suspende, elimina y restaura usuarios y gestiona grupos y sus miembros (OWNER, MANAGER, MEMBER). Pide el ámbito OAuth más limitado posible, como admin.directory.user.readonly o admin.directory.group.member. Para que una cuenta de servicio administre el directorio, asígnale un rol de administrador (nunca Super Admin) antes que la delegación en todo el dominio.
- Workforce Identity Federation permite que los usuarios de un IdP externo compatible con OIDC o SAML 2.0 accedan a Google Cloud con SSO sin sincronizar cuentas ni usar GCDS. Se configura con grupos de identidades de personal a nivel de organización y proveedores con asignaciones de atributos y condiciones de atributos en CEL. Asigna google.subject a un valor inmutable y concede roles con principal:// o principalSet:// (grupo o atributo).

Managing service accounts

- Las cuentas de servicio son principales y recursos. Evita las cuentas de servicio predeterminadas con Editor: aplica iam.automaticIamGrantsForDefaultServiceAccounts e iam.managed.preventPrivilegedBasicRolesForDefaultServiceAccounts. Concede Service Account Token Creator sobre la cuenta concreta, no en el proyecto, y limita el acceso SSH y al servidor de metadatos de las VMs con cuentas privilegiadas.
- Las cuentas de servicio sirven para cargas de trabajo sin intervención de usuarios: asócialas al recurso, usa Workload Identity Federation for GKE en GKE y Workload Identity Federation fuera de Google Cloud. Para actuar en nombre de un usuario usa OAuth 2.0; en desarrollo local, credenciales de usuario o suplantación. No uses cuentas de servicio en apps cliente ni en la consola, y no pueden ser propietarias de recursos de Workspace.
- Crea cuentas de servicio de un solo uso con gcloud iam service-accounts create y concede Service Account User (iam.serviceAccounts.actAs) sobre la cuenta a quien deba asociarla a recursos. Deshabilítala antes de eliminarla: una cuenta recreada con el mismo nombre es otra identidad sin los enlaces de IAM. iam.managed.disableServiceAccountCreation bloquea su creación, y su uso entre proyectos depende de iam.disableCrossProjectServiceAccountUsage.
- Las claves de cuenta de servicio son la excepción: aplica iam.managed.disableServiceAccountKeyCreation en la raíz de la organización con excepciones por proyecto, e iam.serviceAccountKeyExposureResponse en DISABLE_KEY. Si una clave se ve comprometida, deshabilitarla no revoca los tokens ya emitidos: deshabilita la cuenta o aplica una política de denegación. Revisa el uso con Activity Analyzer y Cloud Monitoring antes de deshabilitar y eliminar.
- Las credenciales de corta duración (tokens de acceso OAuth 2.0, tokens de ID de OIDC, JWT y blobs firmados) se crean con la Service Account Credentials API y son más seguras que las claves de cuenta de servicio. El rol Service Account Token Creator permite crearlas; para solo tokens de ID basta el rol Service Account OpenID Connect Identity Token Creator. Los tokens no traen token de actualización y la autosuplantación está prohibida.

Managing authentication

- Creating a password and session management policy for user accounts
- Setting up Security Assertion Markup Language (SAML) and OAuth
- Configuring and enforcing 2-step verification

Managing and implementing authorization controls

- La separación de funciones evita que un solo principal tenga todos los permisos para una acción maliciosa: en Cloud KMS se separan administradores y usuarios de claves, y los roles Project IAM Admin o Folder IAM Admin permiten gestionar políticas sin acceso directo a los datos. Privileged Access Manager concede roles de forma temporal con justificación y aprobación, pero no revoca las vinculaciones permanentes existentes.
- En Cloud Storage, IAM y las ACL actúan en paralelo: basta con que uno conceda acceso, así que una ACL pública puede exponer un objeto aunque IAM sea restrictivo. El acceso uniforme a nivel de bucket desactiva las ACL, es necesario para carpetas gestionadas, condiciones de IAM en el bucket e identidades federadas, puede exigirse con una política de la organización y solo puede revertirse durante 90 días.
- Las condiciones de IAM (CEL) conceden roles solo si se cumple una expresión, como una fecha con request.time o un prefijo con resource.name acotado por resource.type; no valen para roles básicos heredados ni allUsers. Las políticas de denegación se adjuntan a organizaciones, carpetas o proyectos, se evalúan antes que las de permisos, admiten excepciones y conjuntos de principales, y sus condiciones solo usan etiquetas.
- Concede el rol predefinido o personalizado más limitado en el ámbito más pequeño que baste: un tema de Pub/Sub o un conjunto de datos en lugar del proyecto, y la organización solo cuando un equipo necesita acceso a todos los proyectos. Las políticas de permisos se heredan hacia abajo, evita los roles básicos en producción y usa roles como Folder IAM Admin para gestionar accesos sin acceso directo a los recursos.
- Access Context Manager define políticas de acceso que contienen niveles de acceso (IP, identidad, dispositivo, básicos o personalizados en CEL) y perímetros de servicio, pero no aplica nada: lo hacen VPC Service Controls, IAP o las vinculaciones de acceso de Context-Aware Access. Solo hay una política a nivel de organización; las políticas con ámbito delegan carpetas o proyectos, aunque IAP solo admite niveles de la política de la organización.

Defining the resource hierarchy

- Usa una sola organización y carpetas diseñadas según tus necesidades en la nube (entornos, regiones o filiales, responsabilidad por producto), no según el organigrama. Crea carpetas y proyectos desde un pipeline con nombres estandarizados, controla quién tiene Project Creator (que por defecto tiene todo el dominio) y usa roles como Folder Mover y etiquetas heredables para gestionar a escala.
- Una política de la organización aplica una restricción en una organización, carpeta o proyecto y la heredan sus descendientes. Las restricciones gestionadas (iam.managed.*) sustituyen a las heredadas y admiten Policy Simulator y el modo de prueba; las personalizadas usan CEL sobre campos del recurso con ALLOW o DENY. Las políticas no suelen ser retroactivas y las listas heredadas se combinan con inheritFromParent.
- Las políticas de permisos, de denegación y de la organización se heredan desde la organización y las carpetas hasta los proyectos y sus recursos. Las de permisos son aditivas: un proyecto no puede quitar un rol heredado y, para bloquearlo, se usa una política de denegación, que se evalúa antes y admite principales exentos. Mover un proyecto cambia lo que hereda, y los roles personalizados no se crean en carpetas.

2. Securing communications and establishing boundary protection

22–22%

Designing and configuring perimeter security

- Cloud NGFW agrupa reglas en políticas de cortafuegos jerárquicas (organización o carpetas, no anulables desde abajo y con goto_next para delegar), políticas de red globales y regionales, y reglas de cortafuegos de VPC; las etiquetas seguras están controladas por IAM. El reenvío TCP de IAP da SSH o RDP sin IP externas, los balanceadores de aplicaciones validan mTLS con una configuración de confianza y CA Service gestiona CA privadas.
- La inspección de capa 7 de Cloud NGFW Enterprise usa endpoints de cortafuegos zonales asociados a la red de VPC, grupos de perfiles de seguridad (threat-prevention para IPS, url-filtering para filtrado de URL) y reglas de políticas de cortafuegos con la acción apply_security_profile_group. Para inspeccionar HTTPS hace falta una política de inspección TLS con un grupo de CA de CA Service. Cloud IDS solo detecta y alerta.
- Las direcciones IP externas se anuncian públicamente; las internas solo son accesibles dentro de la red de VPC, redes emparejadas o conectadas, e incluyen IP públicas de uso privado. Las VM sin IP externa salen a internet con Cloud NAT, que no admite conexiones entrantes no solicitadas, y llegan a las API de Google con el acceso privado a Google. Restricciones como compute.vmExternalIpAccess limitan las IP externas y no son retroactivas.
- Cloud Armor aplica políticas de seguridad a solicitudes entrantes en los balanceadores de carga: las de backend admiten reglas WAF preconfiguradas basadas en OWASP CRS, reCAPTCHA, limitación y bloqueo por frecuencia; las de borde filtran antes de la caché y son las únicas para buckets de backend. Conviene probar las reglas en modo de vista previa y empezar con sensibilidad baja antes de aplicarlas.
- Secure Web Proxy controla el tráfico web saliente (HTTP y HTTPS) con denegación predeterminada y reglas por cuenta de servicio, etiqueta segura y host de destino. Se despliega en el proyecto host con una subred PRIVATE y una subred de solo proxy por región, en modo explícito o de siguiente salto. Con inspección TLS y un grupo de CA de CA Service puede filtrar rutas completas de URL.

Configuring boundary segmentation

- La VPC compartida centraliza redes y cortafuegos en el proyecto host: compute.networkUser por subred limita dónde despliega cada equipo, y networkAdmin y securityAdmin separan red y cortafuegos. VPC Network Peering solo intercambia rutas, no es transitivo ni comparte reglas de cortafuegos, y compute.restrictVpcPeering limita con quién se empareja. Las políticas de cortafuegos jerárquicas imponen reglas que los proyectos no pueden anular.
- Para aislar los niveles de una aplicación se usan reglas de entrada por flujo permitido con cuentas de servicio o etiquetas seguras (GCE_FIREWALL, con control de IAM) en lugar de etiquetas de red, que cualquiera con permiso para editar la VM puede cambiar. Las políticas jerárquicas aplican reglas en carpetas con cuentas de servicio de destino, y Private Service Connect expone un único servicio de otra VPC sin intercambiar rutas.
- VPC Service Controls crea perímetros de servicio que impiden copiar datos de servicios como BigQuery o Cloud Storage a recursos externos, incluso con permisos de IAM válidos. Las reglas de entrada y salida conceden accesos concretos por identidad, origen, servicio y método, también entre organizaciones; los puentes solo unen perímetros de la misma organización. El modo de prueba registra infracciones sin bloquearlas antes de aplicar cambios.

Establishing private connectivity

- La VPC compartida conecta proyectos de servicio a la red de un proyecto host con administración central; compute.networkUser se puede conceder por subred y restricciones como compute.restrictSharedVpcSubnetworks limitan su uso. El emparejamiento de redes de VPC no es transitivo ni intercambia reglas de cortafuegos. Los hosts locales llegan a las APIs de Google con DNS hacia private o restricted.googleapis.com y rutas anunciadas en Cloud Router.
- HA VPN cifra con IPsec el tráfico entre la red local y la VPC a través de internet, con dos interfaces por puerta de enlace. Cloud Interconnect no cifra el tráfico de forma predeterminada: MACsec cifra en capa 2 entre tu router y el perímetro de Google, y HA VPN sobre Cloud Interconnect añade IPsec sobre los adjuntos de VLAN sin pasar por internet. La restricción compute.managed.allowedVlanAttachmentEncryption puede exigir adjuntos IPsec.
- El acceso privado a Google se habilita por subred para VMs sin IP externa y exige rutas con la puerta de enlace de internet predeterminada como siguiente salto. restricted.googleapis.com solo permite APIs compatibles con VPC Service Controls y private.googleapis.com casi todas. Los endpoints de Private Service Connect usan una IP interna propia, accesible desde local, con los paquetes all-apis o vpc-sc.
- Public NAT, configurado en un Cloud Router de la región, da salida a internet a recursos sin IP externa y nunca admite conexiones entrantes no solicitadas; con asignación manual se comparten IP de origen fijas. Una IP externa en la interfaz siempre tiene prioridad sobre la NAT. Las reglas de cortafuegos se aplican a las VMs y las de salida se evalúan antes de la NAT; compute.restrictCloudNATUsage limita qué subredes usan Cloud NAT.

3. Ensuring data protection

23–23%

Protecting sensitive data and preventing data loss

- El servicio de descubrimiento de Sensitive Data Protection perfila de forma continua datos de una organización, carpeta o proyecto; los trabajos de inspección analizan una ubicación concreta. Para desidentificar hay redacción, sustitución, enmascaramiento y seudonimización: AES-SIV y cifrado con conservación de formato son reversibles, el hash criptográfico no. La clave envuelta con Cloud KMS es la opción preferida.
- En BigQuery, las vistas autorizadas comparten un subconjunto sin dar acceso al conjunto de origen, las etiquetas de política controlan columnas y las políticas a nivel de fila filtran filas por lista de beneficiarios. En Cloud Storage, el acceso uniforme a nivel de bucket desactiva las ACLs y la prevención del acceso público bloquea allUsers. Cloud SQL admite autenticación de base de datos de IAM con roles/cloudsql.instanceUser.
- Secret Manager guarda secretos versionados cifrados en reposo y en tránsito. Se recomienda conceder roles/secretmanager.secretAccessor por secreto, referenciar números de versión en lugar de latest, deshabilitar antes de destruir y usar la API con bibliotecas de cliente en vez de variables de entorno. La rotación programada envía SECRET_ROTATE a Pub/Sub, y AccessSecretVersion queda en los registros de acceso a datos.
- Cualquier proceso que consulte el servidor de metadatos puede leer todos sus valores, así que los secretos van en Secret Manager y los procesos que no deban acceder se aíslan. En Shielded VM, el endpoint HTTPS evita la suplantación y la manipulación. OS Login sustituye las claves SSH en metadatos y compute.managed.requireOsLogin lo exige; block-project-ssh-keys bloquea las claves del proyecto en una VM.

Managing encryption at rest, in transit, and in use

- El cifrado predeterminado de Google cifra todos los datos en reposo con AES-256 sin configuración, pero no permite gestionar las claves ni ver su uso. CMEK con Cloud KMS o Cloud HSM da control de rotación, destrucción (crypto-shredding) y registros de acceso, y Autokey lo automatiza. Cloud EKM mantiene el material de clave en un gestor externo, nunca en Google Cloud; por VPC ofrece mejor disponibilidad que por internet.
- Cloud KMS ofrece niveles de protección SOFTWARE, HSM (Cloud HSM multiinquilino), HSM_SINGLE_TENANT (particiones dedicadas que administras tú) y EXTERNAL o EXTERNAL_VPC (Cloud EKM, clave fuera de Google). Todos sirven como CMEK y con las mismas API; las claves de Cloud HSM tienen declaración de atestación, y la restricción cloudkms.allowedProtectionLevels limita qué niveles se pueden crear en una carpeta.
- Las claves CMEK se crean a mano o con Cloud KMS Autokey. La rotación crea una versión principal nueva, pero no vuelve a cifrar datos ni inhabilita versiones antiguas; antes de destruir una versión conviene inhabilitarla y vigilar los registros. Una versión importada no pasa a ser principal sola. En Cloud EKM, solo las claves coordinadas por VPC rotan automáticamente, y revocar el acceso en el EKM corta el uso de la clave.
- El tráfico por IP internas entre VM de una VPC o de VPC emparejadas se cifra y autentica automáticamente; por IP externas no. Para cifrar en la capa de aplicación se usa cifrado de sobre: una DEK local por escritura, encapsulada con una KEK de Cloud KMS. CSEK solo se aplica por objeto; para claves fuera de Google como predeterminadas se usa Cloud EKM, y GKE puede cifrar los Secrets con una clave de Cloud KMS.
- Object Lifecycle Management aplica reglas con acciones Delete, SetStorageClass o AbortIncompleteMultipartUpload cuando un objeto cumple todas las condiciones (age, numNewerVersions, daysSinceNoncurrentTime, matchesPrefix…). Una configuración nueva sustituye a todas las reglas existentes. Delete no actúa sobre objetos con retenciones o con la política de retención sin cumplir, pero sí elimina objetos de un bucket bloqueado ya vencidos.

Securing AI workloads

- Para evitar fugas involuntarias de datos o modelos: minimiza y desidentifica los datos de entrenamiento con Sensitive Data Protection, analiza prompts y respuestas con Model Armor (plantillas de entrada y salida separadas, modo inspeccionar y bloquear) y aísla en proyectos distintos los modelos que no todos deben desplegar. AI Protection en Security Command Center inventaría modelos y detecta los que no protege Model Armor.
- En IaaS (VM de Compute Engine propias) asumes casi toda la seguridad: cuentas de servicio dedicadas de mínimo privilegio, Shielded VM o Confidential VM (también con GPU NVIDIA), CMEK y parches. En PaaS, Agent Platform gestiona las VM de entrenamiento; tú asocias cuentas de servicio personalizadas a cada trabajo, usas CMEK, VPC Service Controls y una interfaz de Private Service Connect o IP privada para no exponerlo.
- Controles de Gemini Enterprise Agent Platform: roles personalizados de mínimo privilegio (por ejemplo, solo aiplatform.endpoints.predict), VPC Service Controls para impedir la exfiltración de datos y modelos (con niveles de acceso y reglas de entrada para orígenes autorizados), CMEK, floor settings de Model Armor para analizar todas las llamadas de un proyecto y restricciones como vertexai.allowedModels o ainotebooks.disableRootAccess.

4. Managing operations

19–19%

Automating infrastructure and application security

- Artifact Analysis analiza imágenes de Artifact Registry automáticamente al subirlas (una vez por digest) y las mantiene al día con análisis continuo; publica cambios en el tema de Pub/Sub container-analysis-occurrences-v1. On-Demand Scanning analiza imágenes locales o del registro desde gcloud y, en Cloud Build, permite fallar la compilación antes de subirla si hay gravedades bloqueadas (indica todas, por ejemplo CRITICAL|HIGH).
- Binary Authorization aplica una política por proyecto (regla predeterminada y, en GKE, reglas específicas) que puede exigir atestaciones firmadas, verificadas por attestors con claves que pueden residir en Cloud KMS. El modo de prueba solo registra, breakglass permite despliegues de emergencia que quedan en Cloud Audit Logs, y en Cloud Run conviene exigirlo con la restricción run.allowedBinaryAuthorizationPolicies.
- Las imágenes personalizadas reforzadas se agrupan en familias y se retiran con gcloud compute images deprecate (DEPRECATED solo avisa; OBSOLETE impide crear VMs). La restricción compute.trustedImageProjects limita los proyectos de imágenes de arranque. VM Manager aplica parches programados con el agente de OS Config y las políticas de SO mantienen el estado deseado de paquetes y agentes.
- Las restricciones personalizadas de la política de la organización usan CEL sobre campos del recurso para bloquear creaciones o actualizaciones; conviene probarlas en modo de prueba. Los módulos personalizados de Security Health Analytics detectan configuraciones incorrectas en recursos existentes. Una postura de seguridad agrupa controles preventivos y de detección, se despliega por niveles de la jerarquía y notifica la deriva como hallazgos.

Configuring logging, monitoring, and detection

- Los registros de flujo de VPC muestrean y agregan conexiones (no ven los paquetes de entrada denegados), el registro de reglas de cortafuegos se activa por regla y Packet Mirroring copia paquetes completos a recolectores. Cloud IDS analiza tráfico duplicado y solo avisa, mientras que la prevención de intrusiones de Cloud NGFW bloquea en línea. Observability Analytics permite agregar registros con SQL.
- Los registros de actividad de administración y de eventos del sistema siempre se escriben; los de acceso a datos deben habilitarse y, si se activan en la organización, los proyectos no pueden desactivarlos. Los receptores agregados (interceptores o no) centralizan registros, Pub/Sub sirve para SIEM externos, los segmentos bloqueados fijan la retención y los ajustes predeterminados fijan ubicación y CMEK.
- Security Command Center reúne hallazgos de Event Threat Detection, Container Threat Detection y Virtual Machine Threat Detection; las exportaciones continuas a Pub/Sub permiten respuestas automáticas y las reglas de silenciamiento dinámicas ocultan hallazgos de forma temporal. Para responder conviene conservar discos para el análisis forense y desactivar las cuentas comprometidas antes de eliminarlas.
- Logs Viewer no muestra los registros de acceso a datos de _Default; para eso está Private Logs Viewer. Las vistas de registros, con roles/logging.viewAccessor en su política, limitan qué entradas ve cada usuario, y los campos restringidos con Logs Field Accessor ocultan campos concretos, aunque BigQuery no los respeta. Los receptores escriben con su identidad de escritura y CMEK se fija al crear el segmento.
- Para enviar registros a un SIEM externo se crea un receptor agregado en la organización o carpeta con destino un tema de Pub/Sub, y se concede a la identidad de escritura del receptor el rol de publicación. Los receptores no reenvían entradas antiguas: para el histórico se copian los registros del segmento a Cloud Storage. El patrón de envío con Dataflow evita claves de cuenta de servicio y guarda el token del SIEM en Secret Manager.

5. Supporting compliance requirements

11–11%

Adhering to regulatory and industry standards requirements for the cloud

- Cada requisito normativo se traduce en controles técnicos por capa: Bucket Lock y el modo de auditoría detallada para registros inmutables en almacenamiento; seudonimización con Sensitive Data Protection, porque el cifrado en reposo no tokeniza datos como el PAN; restricciones como sql.restrictPublicIp en red; Confidential VM, Shielded VM y OS Login en cómputo; y gcp.restrictNonCmekServices con gcp.restrictCmekCryptoKeyProjects para exigir CMEK.
- En la responsabilidad compartida, Google siempre protege la infraestructura y la red subyacentes, y el cliente siempre responde de sus políticas de acceso y sus datos. En IaaS el cliente asume casi todo, como el sistema operativo y los paquetes; en PaaS Google asume más controles, y en SaaS casi todos. Los controles heredados sirven como evidencia ante auditores, y el destino compartido añade blueprints seguros y el Risk Protection Program.
- Assured Workloads aplica límites de datos con controles de residencia, acceso y personal; sus marcos admiten modo detectivo antes del preventivo en carpetas existentes. gcp.resourceLocations, mejor con grupos como in:eu-locations, limita dónde se crean recursos nuevos. Access Transparency registra el acceso de Google, Access Approval exige aprobarlo antes y Key Access Justifications decide el uso de claves según la justificación.
- Delimita el entorno regulado aislando las cargas dentro del alcance en proyectos dedicados, separados de producción, desarrollo y QA, y localiza los datos sensibles con el descubrimiento de Sensitive Data Protection. Google responde de la infraestructura que gestiona; el SO, las aplicaciones, los accesos y los datos son tuyos, y un BAA solo cubre los servicios incluidos.
- Cada requisito se traduce en un control: segmentación con reglas de cortafuegos explícitas y su registro, perímetros de VPC Service Controls contra la exfiltración, registros de acceso a datos habilitados en la carpeta u organización, Access Transparency para el personal de Google y receptores agregados hacia un almacenamiento bloqueado. Compliance Manager relaciona marcos como PCI DSS con controles de nube.