# EduTech Global

# Pràctica 3: Estratègia de Ciberseguretat al Núvol

---

**Assignatura:** Control d'Accés
**Professor/a:** Joan Caubet
**Alumne:** Hamza El Haddad Sabri

---

# ÍNDEX

# Introducció

En l'actual ecosistema tecnològic, la migració al núvol s'ha convertit en un pas estratègic per a moltes organitzacions que busquen escalabilitat i eficiència. EduTech Global, plataforma d'aprenentatge en línia amb dades sensibles d'estudiants i professors, no és una excepció.

**Objectiu de la pràctica:** Definir una estratègia integral de ciberseguretat al núvol per a EduTech Global, utilitzant Google Cloud com a referència. L'estratègia combinarà mesures, eines, polítiques i procediments per protegir les dades, les aplicacions i la infraestructura allotjades al núvol. S'abordaran aspectes clau com la identificació dels actius i serveis cloud de l'empresa, l'anàlisi de riscos específics d'entorns cloud, la gestió d'identitats i accessos (IAM), la protecció de dades, la seguretat de la infraestructura, la detecció i resposta a incidents en entorns cloud, i finalment s'establirà una **política bàsica de seguretat al núvol** que guiï aquestes mesures.

Cal destacar que, a diferència de l'entorn tradicional on EduTech tenia control complet de la infraestructura física, en el núvol s'aplica un **model de responsabilitat compartida**: el proveïdor (Google) gestionarà la seguretat de la infraestructura bàsica (centres de dades, maquinari, xarxa física), mentre que EduTech Global és responsable de configurar correctament la seguretat dels seus serveis, aplicacions i dades al núvol. Amb això en ment, a continuació s'identifiquen els actius cloud de l'organització i els riscos associats, i es despleguen les mesures de seguretat necessàries per afrontar-los.

# Infraestructura Cloud d'EduTech Global: Actius i Serveis

Abans de definir les mesures de seguretat, és essencial inventariar i comprendre la **infraestructura cloud** d'EduTech Global, és a dir, quins actius i serveis s'hi desplegaran. EduTech Global planeja migrar la major part dels sistemes actuals al Google Cloud Platform (GCP), aprofitant els serveis gestionats que ofereix. A continuació es presenten els principals recursos al núvol que conformaran l'arquitectura de la plataforma educativa, amb la seva funció i importància:

| Recurs Cloud | Descripció i Ús a EduTech Global | Criticitat |
|---|---|---|
| **Entorn Google Cloud (Organització i Projectes)** | Conta de Google Cloud de l'empresa que agrupa tots els recursos (projectes, usuaris, permisos). L'accés administrador a aquest entorn permet gestionar la resta d'actius. | Màxima (crític) |
| **Servidors d'aplicació (Google Compute Engine)** | Màquines virtuals que allotgen el portal web i aplicacions educatives d'EduTech. S'executen els serveis de front-end i lògica de negoci. | Alt (servei essencial) |
| **Base de dades d'usuaris (Cloud SQL)** | Servei de base de dades relacional gestionat que emmagatzema informació sensible: dades personals d'estudiants i professors, qualificacions, etc. | Màxima (dades crítiques) |
| **Emmagatzematge d'objectes (Cloud Storage)** | Repositoris d'objectes fitxers: materials didàctics, continguts multimèdia dels cursos, còpies de seguretat i documents. Pot contenir tant informació pública (p. ex. vídeos educatius) com dades privades (backups). | Mitjana (variable segons dades) |
| **Xarxa Virtual (VPC i Subxarxes)** | Xarxa privada virtual que connecta els components anteriors. Inclou subxarxes segregades (per exemple, una per als servidors d'aplicació i una de privada per a la base de dades) i rutes de comunicació internes. | Alt (exposició controlada) |

| | | |
|---|---|---|
| **Serveis d'identitat i IAM** | Sistema de gestió d'identitats integrat: comptes d'usuari Google gestionats via **Cloud Identity** o federats des de l'Active Directory corporatiu, rols IAM de GCP per controlar accés als recursos, comptes de servei per a aplicacions. | Alt (control d'accés) |
| **Eines de Monitorització i Registre (Cloud Logging/Monitoring)** | Serveis de Google per recollir logs d'activitat, mètriques de rendiment i alertes de seguretat dels recursos. Utilitzats per supervisar l'estat i detectar comportaments anòmals. | Alt (detecció d'incidents) |

# Reptes i Riscos de Ciberseguretat associats al Núvol

La computació al núvol introdueix beneficis significatius, però també comporta riscos de ciberseguretat particulars que EduTech Global ha de tenir en compte a l'hora de dissenyar la seva estratègia. Els principals **reptes i riscos** identificats en l'entorn Google Cloud per als actius de l'empresa son els seguents:

- **Amenaces externes i superfícies d'atac ampliades:** En traslladar serveis al núvol, aquests poden estar exposats a Internet (per exemple, el portal web) i per tant són susceptibles a atacs externs tradicionals (injeccions SQL, malware, **DDoS**, escanejos de vulnerabilitats). A més, apareixen vectors nous com atacs als **API de serveis cloud** o als mecanismes d'autenticació de GCP. La infraestructura cloud, si no està ben segmentada, podria permetre que una intrusió en un component (p. ex. un servidor vulnerat) s'estengui lateralment a altres recursos.

- **Compromís de comptes i credencials al núvol:** Els comptes d'usuari amb accés al cloud (administradors de GCP, enginyers, comptes de servei) esdevenen objectius molt atractius. Un **compte privilegiat compromès** (per phishing, credencials febles filtrades, etc.) pot donar a un atacant control total sobre recursos crítics. Cal contemplar el risc de **robatori de claus d'API o credencials de comptes de servei**, que podria permetre accés no autoritzat als sistemes sense passar pels controls tradicionals.

- **Errors de configuració i exposició involuntària de dades:** Un repte important al núvol és assegurar configuracions segures des del primer moment. Per exemple, un bucket de Cloud Storage configurat com a públic per error podria exposar informació confidencial a Internet. De fet, les **males configuracions (misconfigurations)** són una de les principals causes de bretxes de seguretat en entorns cloud. També ho són l'ús de paràmetres per defecte (com contrasenyes predeterminades en VMs o regles de firewall massa obertes). EduTech ha de mitigar aquests riscos aplicant principis de configuració segura i revisions periòdiques.

- **Pèrdua o corrupció de dades sensibles:** Tot i que els proveïdors cloud com Google ofereixen alt nivell de disponibilitat, existeix risc de **pèrdua de dades** si no es fan còpies de seguretat adequades (per exemple, corrupció d'una base de dades sense backup recent). També preocupa la **inadvertida destrucció o modificació** de dades per errors humans o programes maliciosos. La protecció de dades ha d'incloure mecanismes per prevenir pèrdues (còpies de seguretat, control de versions) i per evitar filtracions (xifratge i controls d'accés estrictes).

- **Compliment normatiu i protecció de la privacitat:** EduTech Global manega dades personals d'usuaris (estudiants, professors) subjectes a regulacions de privacitat (GDPR i equivalents). Migrar aquestes dades al núvol pot introduir dubtes sobre on resideixen físicament i com es protegeixen. És un risc no complir requisits legals si, per exemple, es processen dades europees fora de la UE sense garanties. Cal assegurar que la **ubicació dels serveis** cloud i les mesures de protecció de dades

compleixin amb totes les normatives aplicables, i que es mantinguin registres d'auditoria per demostrar-ho.

- **Visibilitat i control reduïts:** En un centre de dades propi, EduTech tenia control directe sobre els servidors, xarxes locals i dispositius de seguretat. Al núvol, part d'aquesta visibilitat es delega al proveïdor. Això pot dificultar detectar certes activitats si no s'utilitzen les eines adequades. Per exemple, sense una configuració acurada de logs i alertes, un incident de seguretat en un entorn cloud podria passar desapercebut més temps. També existeix el repte de la **gestió d'actius "ombra" (shadow IT)**: la facilitat de desplegar nous recursos al núvol pot provocar que departaments facin servir serveis cloud sense coneixement de l'equip de seguretat, creant forats de seguretat fora de supervisió.

- **Dependència del proveïdor i continuïtat de negoci:** Encara que no és una amenaça de ciberatac tradicional, la **dependència en el proveïdor cloud** és un factor de risc a considerar. Una fallada important o indisponibilitat prolongada de Google Cloud podria impactar greument el servei d'EduTech Global. Per això, l'estratègia de seguretat haurà d'incloure plans de **contingència i recuperació** per mantenir la continuïtat del negoci fins i tot davant incidents al núvol (ja siguin ciberatacs o problemes del proveïdor).

# Gestió d'Identitats i Accessos (IAM) al Núvol

La **Gestió d'Identitats i Accessos (Identity and Access Management, IAM)** és un component crític de la seguretat al núvol, ja que controla **qui pot accedir a què** dins l'entorn de Google Cloud. Una estratègia robusta d'IAM garanteix que només els usuaris i sistemes autoritzats puguin realitzar accions específiques, minimitzant el risc d'accés indegut. Per a EduTech Global, es plantegen les mesures següents:

- **Model de privilegis mínims i rols adequats:** En línia amb el principi de *privilegi mínim*, es revisarà la definició de rols IAM a Google Cloud de manera que cada usuari o compte de servei disposi únicament dels permisos estrictament necessaris per a la seva funció. EduTech ja aplicava un model RBAC/ABAC híbrid en sistemes interns (definit a la Pràctica 1); ara es traduirà això a rols de GCP. Per exemple, es definiran rols com ara *administrador del projecte* (amb permisos globals d'administració), *administrador de bases de dades* (amb permisos limitats a Cloud SQL), *desenvolupador* (pot gestionar només recursos de desenvolupament, sense accés a dades en producció), etc. Es farà ús dels **rols predefinits de GCP** sempre que possible (ja que incorporen bones pràctiques) i es crearan **rols personalitzats** només si els predefinits no s'ajusten a les necessitats d'EduTech.

- **Usuaris i grups gestionats centralitzadament:** Totes les identitats (usuaris humans) es gestionaran de manera centralitzada. Idealment, EduTech integrarà el seu directori corporatiu (p. ex. Active Directory existent) amb **Google Cloud Identity** per federar els accessos. Això permet que els comptes dels empleats es sincronitzin i es pugui aplicar Single Sign-On, facilitant la gestió d'alta i baixa d'usuaris de forma consistent. Cada usuari serà assignat al(s) grup(s) corresponent(s) (per exemple, *Departament TI*, *Professors*, *Operacions de seguretat*) i aquests grups s'assignaran als rols IAM definits. D'aquesta manera es simplifica l'administració massiva de permisos: per exemple, un nou tècnic de seguretat que s'uneixi a l'empresa es col·locarà al grup de *Seguretat*, el qual té un rol IAM amb permisos de lectura de logs i auditoria, però no necessàriament permisos operatius sobre recursos de producció.

- **Comptes de servei per a aplicacions i serveis interns:** Els serveis al núvol (com les màquines virtuals del back-end, funcions, etc.) no utilitzaran comptes d'usuari humans per interactuar entre ells, sinó **comptes de servei** dedicats. Un compte de servei de GCP és una identitat no humana associada normalment a aplicacions o components, a la qual també se li poden assignar rols IAM. Es crearà, per exemple, un compte de servei per al servidor d'aplicació que necessita accedir a la base de dades o a un bucket de Cloud Storage; aquest compte tindrà únicament permisos delimitats (p. ex. rol *Cloud SQL Client* sobre la instància de base de dades, i lectura/escriptura només al bucket específic necessari). D'aquesta manera, si un atacant compromet un servidor d'aplicació, només obtindrà els permisos limitats del seu compte de servei, reduint l'abast del potencial dany. Tots els secrets o claus associats a comptes de servei (com claus d'API) es custodiaran de forma segura (idealment evitant claus estàtiques i fent servir **identitat federada** o *Workload*

*Identity* en cas de Kubernetes, per no exposar claus).

- **Autenticació forta i MFA:** Per evitar el **robatori de credencials** i accesos no autoritzats, s'exigirà autenticació forta a tots els usuaris amb accés a recursos cloud. Això inclou **contrasenyes robustes** gestionades segons política corporativa i, sobretot, l'**autenticació multi-factor (MFA)** obligatòria per a comptes amb permisos privilegiats i recomanada per a tots els usuaris. En la pràctica, els administradors i desenvolupadors d'EduTech hauran d'utilitzar un segon factor (com aplicació mòbil d'autenticació o clau de seguretat física) per iniciar sessió a la consola de Google Cloud o als serveis administratius. El fet de requerir MFA redueix dràsticament el risc que un atacant exploti credencials robades, ja que necessitaria també el segon factor. Google Cloud Identity permet implementar MFA fàcilment per a tots els comptes gestionats.

- **Polítiques d'accés condicionals i límits geogràfics/horaris:** Com a part de la política d'IAM, es podrien establir restriccions addicionals sobre **quan** i **des d'on** es pot accedir a recursos crítics. Per exemple, fent ús de **Context-Aware Access** de Google, es pot limitar que només dispositius o xarxes de l'empresa (amb determinades adreces IP o característiques de seguretat) puguin accedir a la consola d'administració o a certs recursos de dades sensibles. També es pot definir que operacions crítiques (p. ex. esborrar una base de dades) només es permetin dins d'una franja horària determinada quan hi ha personal de guàrdia disponible. Aquest tipus de controls contextuals donen una capa més de seguretat adaptada al risc.

- **Auditoria i revisió periòdica de permisos:** Una pràctica necessària serà revisar de forma regular les assignacions de rols IAM. Amb el temps, és possible que alguns usuaris acumulin permisos que ja no necessiten (p. ex. projectes pilot finalitzats, empleats que canvien de rol, etc.). Es planificarà una **auditoria trimestral de permisos** on l'equip de seguretat validarà que cada compte encara requereix els accessos que té. Google Cloud proporciona eines com **Cloud IAM Recommender**, que suggereix reduir permisos si detecta que no s'han utilitzat, la qual cosa pot ajudar a mantenir el principi de privilegi mínim de forma dinàmica. A més, tots els canvis en polítiques IAM quedaran registrats (via Cloud Audit Logs) per si cal investigar accions sospitoses sobre els privilegis.

- **Gestió de claus i comptes privilegiats:** Els usuaris amb rols de màxim privilegi (propietaris de projecte, admins org) seran molt limitats en nombre. S'establirà un procés de **gestió de comptes privilegiats**, on aquests administradors utilitzin comptes separats només per tasques administratives crítiques, mantenint comptes d'usuari normals per a feina quotidiana. Aquests comptes privilegiats estaran subjectes a monitorització addicional. Igualment, qualsevol **clau d'API o credencial especial** que atorgui accés ampli als sistemes estarà emmagatzemada de forma segura (p. ex. utilitzant **Secret Manager** de GCP per guardar secrets necessaris a aplicacions, en comptes de tenir-los en text clar).

# Protecció de Dades al Núvol

La **protecció de les dades** és un pilar central en l'estratègia de seguretat d'EduTech Global, especialment atès que l'empresa gestiona informació personal i acadèmica molt sensible. En entorns cloud, la protecció de dades s'assoleix a través de diverses capes: xifratge robust, controls sobre qui pot veure o modificar la informació, prevenció de filtracions, i polítiques de còpia de seguretat i retenció per evitar pèrdues. EduTech Global adoptarà les següents mesures i controls per salvaguardar les seves dades al núvol:

- **Xifratge de dades en repòs (at rest):** Totes les dades emmagatzemades als serveis cloud es mantindran xifrades en repòs. Google Cloud ja aplica **xifratge per defecte** a discos persistents, bases de dades Cloud SQL i buckets de Cloud Storage, utilitzant claus gestionades per Google. No obstant, per a dades especialment crítiques (per exemple, la base de dades d'usuaris amb informació personal i credencials), EduTech considerarà l'ús de **claus de xifratge gestionades pel client (Customer-Managed Encryption Keys - CMEK)**. Mitjançant Cloud Key Management Service (Cloud KMS), l'empresa pot generar i controlar les seves pròpies claus criptogràfiques per xifrar determinats volums o bases de dades. Això afegeix un nivell de control: fins i tot dins el núvol, només les entitats que tinguin accés a aquestes claus podran desxifrar la informació. Les claus CMEK es desaran en un projecte de seguretat separat i amb accés restringit, i es rotaran periòdicament per complir bones pràctiques criptogràfiques.

- **Xifratge de dades en trànsit (in transit):** Es garantirà que totes les comunicacions i transferències de dades entre components es facin de forma segura. Això implica l'ús obligatori de protocols cifrats com **TLS 1.2+** en totes les connexions: tant els accessos d'usuaris al portal web (https), com les comunicacions internes entre el servidor d'aplicacions i la base de dades, o entre serveis interns. Google Cloud facilita certificats per a balançadors de càrrega, i es poden usar certificats gestionats (Managed SSL) per simplificar el desplegament de TLS al front-end. A més, s'habilitarà l'**autenticació mútua** en serveis interns quan sigui possible (per exemple, si es fan servir microserveis o contenidors, considerar mTLS entre ells) per evitar atacs *man-in-the-middle* en xarxa local virtual. Amb el xifratge en repòs i en trànsit implementat, es compleix un requeriment bàsic de confidencialitat i integritat de les dades tant emmagatzemades com en moviment.

- **Classificació de la informació i controls segons sensibilitat:** EduTech establirà un **esquema de classificació de dades** adaptat al nou entorn cloud. Tot i que a Pràctica 1 ja es mencionaven categories de dades (p. ex. dades personals, financeres, públiques), ara caldrà aplicar-les als recursos cloud. Per exemple, es marcarà la base de dades d'usuaris i els backups com a **dades de nivell alt/confidencial**, els continguts educatius generals com a **dades de nivell moderat** (no públics però tampoc altament sensibles), i el material publicat (com informació de cursos oberts) com a **dades públiques**. Aquesta classificació permetrà aplicar controls diferents: les dades d'alt nivell de confidencialitat requeriran CMEK, registres d'auditoria més exhaustius i restriccions d'accés molt estrictes; mentre que

les dades públiques poden allotjar-se en entorns amb controls estàndard. Tots els usuaris i administradors seran informats i formats en aquesta política de classificació per tal d'assegurar que etiqueten i ubiquen correctament la informació en el lloc adequat del núvol.

- **Prevenció de pèrdua de dades (Data Loss Prevention - DLP):** Per evitar filtracions accidentals o intencionades de dades sensibles, EduTech farà ús d'eines de DLP. En particular, **Google Cloud DLP** ofereix funcionalitats per identificar i ofuscar dades sensibles. Es poden configurar escanejos automàtics dels buckets d'emmagatzematge i fins i tot de cert tràfic de dades per detectar informació com números d'identificació personal, adreces, credencials, etc. Si es detecta que algú intenta pujar a un bucket un conjunt de dades que conté, per exemple, llistats de números d'identitat o qualificacions confidencials en text pla, es podrien aplicar accions automàtiques: avisos de seguretat o fins i tot l'encriptació addicional o eliminació de l'objecte fins que es revisi. El DLP també serà útil per assegurar que quan es comparteixen dades, no hi hagi informació sensible amagada (p. ex. metadades en documents). Les **polítiques de DLP** s'alinearan amb la classificació esmentada: per a dades de nivell alt, regles molt estrictes de no sortida; per a dades moderades, controls moderats; etc.

- **Gestió de còpies de seguretat i retenció de dades:** Un element crític de protecció és garantir la **disponibilitat** de la informació malgrat incidents. S'implementarà un pla de còpies de seguretat regulars per a tots els actius crítics: la base de dades Cloud SQL tindrà activades les **còpies de seguretat automàtiques diàries** (feature nativa de Cloud SQL) i es mantindran múltiples còpies en rotació; a més es realitzaran **instantànies (snapshots)** periòdiques de les màquines virtuals i dels discs persistents que contenen dades crítiques. Aquests backups es desaran en llocs separats: idealment en un altre projecte o fins i tot en una altra regió (per preparar-se contra un desastre regional). Per exemple, backups de la base de dades principal (a Europa) es podrien replicar també en una regió de suport (com Canadà o Àsia) xifrades, per tenir redundància geogràfica. S'establirà una **política de retenció**: mantenir, posem, les còpies diàries dels últims 30 dies i còpies mensuals durant un any, per tal de poder recuperar dades fins i tot si un incident es descobreix tard. Igualment important és provar aquestes còpies: el pla de recuperació de desastres inclourà **proves de restauració** semestrals per assegurar que les backups són vàlides i que l'equip sap com procedir ràpidament en cas necessari (per exemple, simular la recuperació d'un bucket sencer o el **failover** de la base de dades a una rèplica de seguretat).

- **Control d'accés a les dades i logs d'auditoria:** Complementant l'IAM general, es definiran controls d'accés específics a dades. Per exemple, dins Cloud SQL cada usuari de base de dades tindrà els privilegis SQL mínims (separant comptes d'aplicació i comptes d'administració de la BD). Als buckets de Cloud Storage, s'utilitzaran etiquetes i **polítiques IAM per objecte** si cal per restringir qui pot llegir o escriure fitxers concrets. Totes les accions rellevants sobre dades sensibles (lectures massives, exports, esborrats) quedaran registrades via **Cloud Audit Logging**.

Aquests registres s'emmagatzemaran de manera segura i s'integraran amb els sistemes de monitorització de seguretat per generar alertes en cas d'accessos inusuals (per exemple, si un usuari accedeix de cop a milers de registres de la base de dades fora del seu horari habitual, saltaria una alerta de possible exfiltració).

- **Protecció de dades en dispositius client:** Tot i que el focus d'aquesta estratègia és l'entorn cloud, cal recordar que les dades finalment arriben a dispositius d'usuaris (ordinadors de personal, portàtils de professors, etc.). Per tancar el cicle de protecció, EduTech mantindrà polítiques de **seguretat del punt final**: exigir dispositius xifrats i amb contrasenya per accedir a dades sensibles, i utilitzar canals segurs (VPN o TLS) per connexions remotes. D'aquesta forma es garanteix que la protecció de la dada es manté des del servidor al núvol fins a l'usuari final.

Amb aquestes mesures, EduTech Global assegura la **confidencialitat, integritat i disponibilitat** de les seves dades al núvol. Encara que un atacant aconseguís travessar alguns controls de xarxa o accedir a sistemes, es trobaria amb dades xifrades i amb sistemes de detecció que alertaran de qualsevol ús indegut (per exemple, accedir a una gran quantitat de registres personals). A més, en cas de desastre o sabotatge, les còpies de seguretat garantirien que l'activitat de l'empresa pot recuperar-se.

# Protecció de la Infraestructura Cloud

La **infraestructura cloud** d'EduTech Global comprèn tant els components de computació (màquines virtuals, eventualment contenidors) com els elements de xarxa i serveis que els connecten. Protegir la infraestructura significa assegurar-se que aquests components estan fortificats contra atacs, ben configurats i que el seu comportament està restringit segons el previst. A continuació es detallen les mesures per protegir la infraestructura al núvol:

- **Segmentació de la xarxa i arquitectura segura:** S'implementa una arquitectura de xarxa al núvol similar als principis definits a la Pràctica 1 per a l'entorn local, adaptada a GCP. Es crearà una **VPC (Virtual Private Cloud)** principal per a EduTech Global, dividida en **subxarxes** separades per zones de seguretat. Per exemple, una subxarxa *frontend* per als servidors d'aplicacions web (amb accés a internet públic controlat a través d'un equilibrador de càrrega) i una subxarxa *backend* privada per a la base de dades i sistemes interns, sense accés directe des d'Internet. La comunicació entre subxarxes es limitarà estrictament: només els servidors d'aplicació poden comunicar-se amb la base de dades pel port específic (p. ex. MySQL 3306) i res més. Aquesta segmentació conté l'abast d'un possible intrús; fins i tot si aconsegueix comprometre un servidor del frontend, no tindrà via lliure cap a altres sistemes crítics sense superar altres controls.

- **Controls de trànsit i firewalls:** Google Cloud proporciona **firewall a nivell de VPC**, on es poden definir regles d'entrada i sortida. EduTech configurarà regles de **tallafocs** restrictives: per defecte tot el trànsit entrant estarà denegat excepte aquells ports/serveis explícitament necessaris. Per exemple, s'obriran únicament els ports 80/443 cap als servidors web (permetent HTTP/HTTPS dels usuaris) i es podrien limitar fins i tot a través d'un *load balancer* específic. El port de base de dades no estarà exposat a Internet; només acceptarà connexions de la IP interna dels servidors d'aplicació (o millor, s'utilitzarà el servei de **Cloud SQL Proxy** que evita connexions directes). Pel trànsit sortint, es revisarà què necessiten els serveis: es pot denegar sortida a Internet des de la base de dades (que no n'hauria de fer) i permetre només la sortida des dels servidors web a determinades API externes si escau. Aquest enfocament de *zero trust network* (xarxa de confiança zero) assumeix que cap component ha de confiar directament en la xarxa: tot ha d'estar autoritzat. A més, s'activaran **logs de firewall** per tenir visibilitat de connexions bloquejades i per auditar intents d'intrusió.

- **Accés privat als serveis i aïllament d'instàncies:** Quan sigui possible, es faran servir **serveis privats** per connectar els recursos. Per exemple, s'activarà **Private Google Access** de manera que les instàncies a la VPC puguin accedir a les API de Google Cloud (com Cloud Storage, Cloud SQL) sense haver de sortir a Internet, sinó a través de la xarxa interna de Google. Això evita exposar trànsit sensible a la xarxa pública i mitiga certs atacs de xarxa. Igualment, per administrar els servidors, es preferirà utilitzar **IAP (Identity-Aware Proxy)** o sessions de **SSH restringides** en lloc d'obrir ports SSH a Internet: l'IAP permet als administradors connectar-se a les instàncies de manera segura via túnels autenticats amb comptes Google (subjectes

a MFA), sense tenir cap port d'administració públic actiu.

- **Protecció contra atacs de Denegació de Servei i web:** El portal EduTech Global, en estar accessible als usuaris mundials, pot ser objectiu de **DDoS** o d'atacs web (p. ex. injeccions en formularis). Per això, s'implementaran serveis de protecció específics com **Google Cloud Armor**, que actua com a **WAF (Web Application Firewall)** i escut de DDoS. Cloud Armor es col·loca davant de l'equilibrador de càrrega i pot filtrar trànsit maliciós conegut (per exemple, bloquejant peticions amb patrons d'injecció SQL, o limitant el nombre de peticions per segon per IP per mitigar DDoS de volum). A més, GCP de per sí absorbeix gran part de DDoS de xarxa amb la seva infraestructura global, però Cloud Armor afegeix regles personalitzables a nivell d'aplicació. Aquesta capa addicional és important per assegurar disponibilitat del servei fins i tot sota atac, i complementa les mesures de codi segur que ja es prenen en el desenvolupament de l'aplicació (ex. validació d'entrades per evitar injeccions, etc.).

- **Gestió de pegats i actualitzacions contínues:** Un avantatge d'alguns serveis gestionats (com Cloud SQL) és que Google aplica actualitzacions de seguretat al software base automàticament. No obstant, les màquines virtuals i qualsevol programari instal·lat a sobre són responsabilitat d'EduTech. Es definirà un procés de **gestió de pegats** regular per a aquestes instàncies: s'habilitaran **actualitzacions automàtiques de seguretat** en sistemes operatius on sigui possible (per exemple, usant imatges de **Container-Optimized OS** o **Ubuntu Pro** que suporten autopatching per a vulnerabilitats crítiques). Per als components que no es puguin actualitzar automàticament sense risc (p. ex. canvis que requereixen proves), es programaran actualitzacions mensuals manualment: l'equip de TI mantindrà un calendari on, un cop al mes, totes les instàncies es revisen i s'apliquen pegats pendents del sistema operatiu i middleware (servidors web, etc.), aprofitant horaris de menys activitat per reiniciar si cal. Abans d'això, es provaran els pegats en un entorn de *staging*. També es mantindrà actualitzat el codi de l'aplicació i les llibreries de tercers (frameworks, etc.) per evitar que vulnerabilitats conegudes en versions antigues siguin explotades. En entorns containeritzats, s'automatitzarà l'escanneig d'imatges per evitar imatges amb vulnerabilitats (per exemple, utilitzant **Container Analysis** de Google per analitzar les imatges al Container Registry, i habilitant **Binary Authorization** en GKE si s'usa, així només es despleguen imatges verificades).

- **Còpies de seguretat de la infraestructura i plans de recuperació:** Ja s'ha comentat l'aspecte de les dades, però la infraestructura també requereix preparació per a desastres. A més de backups de dades, es conservaran **imatges de sistema o configuracions** de la infraestructura: templates d'instàncies, scripts d'instal·lació, definicions d'infraestructura com a codi (si s'utilitza Terraform o Deployment Manager per desplegar recursos). Això permetria reconstruir ràpidament la infraestructura en un projecte nou o regió diferent si fos necessari (per exemple, si un atac ransomware encriptés màquines virtuals en producció, es podria redeployar instàncies noves a partir de les imatges netes i restaurar-hi les dades dels backups). Paral·lelament, es

considerarà tenir **entorns de prova** que repliquin (a menor escala) la configuració de producció per testejar tant actualitzacions com procediments de recuperació, sense tocar l'entorn real fins estar segurs.

- **Hardening i configuració segura per defecte:** Cada recurs es desplegarà seguint *benchmarks* de seguretat reconeguts. Per exemple, s'aplicaran les recomanacions del **CIS Benchmark for Google Cloud** en la configuració inicial: deshabilitar comptes/demos innecessaris, assegurar que tots els discos estan xifrats, activar la integritat de logs, etc. En crear una nova màquina virtual, s'executaran scripts de *hardening* (configuració segura) que configuren el firewall del sistema operatiu, inhabiliten serveis no utilitzats i estableixen polítiques estrictes (com bloqueig després de diversos intents fallits d'accés, etc.). De forma similar, a la base de dades Cloud SQL s'activarà la **requiring SSL connections** i es vetllarà perquè només accepti connexions autenticades i des de xarxa permesa. L'objectiu és que qualsevol nou component al núvol parteixi d'una postura de seguretat òptima des del primer moment, minimitzant la necessitat de retoc manual posterior i reduint la possibilitat d'oblit de configuracions importants.

- **Vigilància de recursos no controlats:** Per combatre la problemàtica del *shadow IT*, es farà servir l'eina de **Cloud Asset Inventory** de GCP i es realitzaran escanejos periòdics de recursos en tots els projectes de l'organització EduTech. Això ajudarà a detectar si apareix algun recurs no previst (per exemple, algú crea una instància de VM fora del procediment habitual). A més, amb **Organizational Policy** de GCP es pot impedir directament certes accions: per exemple, es pot imposar una política perquè **només comptes de servei específics** puguin crear determinats recursos, o perquè **no es puguin crear** determinats tipus de recursos considerats de risc (com VMs públiques sense IP privada, etc.). Aquestes polítiques actuaran de salvaguarda per evitar configuracions o desplegaments que vagin en contra de l'estratègia de seguretat establerta.

Mitjançant aquestes accions, la infraestructura cloud d'EduTech Global quedarà **fortificada** contra un ampli ventall d'amenaces. La segmentació de xarxa i els firewalls limiten l'exposició; les eines com Cloud Armor aporten defenses específiques contra atacs sofisticats; el manteniment proactiu de pegats i config. segura redueix vulnerabilitats explotables; i les polítiques d'organització i vigilància eviten desviaments no autoritzats de l'estàndard de seguretat.

Així com la protecció en prevenció és essencial, és igualment crític poder **detectar i respondre** ràpidament si es produeix un incident de seguretat.

# Detecció i Resposta a Incidents al Núvol

Cap sistema és infal·lible, i per molt robustos que siguin els controls preventius, sempre existeix la possibilitat d'un incident de seguretat. És per això que l'estratègia al núvol d'EduTech Global incorpora fortes capacitats de **detecció d'amenaces i resposta a**

**incidents**, aprofitant les eines natives de Google Cloud i integrant-les amb els processos de seguretat de l'empresa. Els objectius són: detectar el més aviat possible qualsevol activitat anòmala o maliciosa en els recursos cloud, respondre de manera eficient per contenir l'incident, i aprendre'n per millorar la postura de seguretat, d'aquesta manera les accions que s'han de dur a terme són les següents:

- **Registre unificat d'esdeveniments i monitorització contínua:** Tots els serveis i recursos cloud generen **logs** que poden ser valuosos per a la seguretat. EduTech habilitarà de forma sistemàtica els **Cloud Audit Logs** per a cada projecte i servei en ús. Aquests registres inclouen esdeveniments com: accessos al sistema (qui ha accedit a quina dada), canvis en la configuració (ex. modificació d'un ajust de firewall o d'un rol IAM), esdeveniments administratius (creació o esborrat de recursos), etc. Paral·lelament, es recolliran els logs específics de les aplicacions (registre d'accessos a la web, errors d'aplicació, etc.) enviant-los a **Cloud Logging**. Centralitzar tots aquests **registres** en una plataforma permet correlacionar esdeveniments. S'establiran **dashboards de monitorització** mitjançant **Cloud Monitoring** per vigilar mètriques clau tant de rendiment (p. ex. ús de CPU, memòria, per detectar comportaments anòmals d'un servidor possiblement compromès) com de seguretat (nombre d'intents fallits d'autenticació, volum de trànsit a bases de dades, etc.). La monitorització contínua assegura que l'equip de seguretat disposi de **visibilitat en temps real** del que succeeix en l'entorn cloud.

- **Alertes i detecció automàtica d'amenaces:** Sobre la base dels logs i mètriques recollits, es configuraran **alertes automàtiques** per a indicadors de possible incident. Per exemple:

    - Alerta si es concedeix un permís IAM d'alt privilegi a un usuari per primera vegada o fora del procediment establert (podria indicar elevació no autoritzada).

    - Alerta si un servidor inicia un trànsit sortint inusual cap a una adreça IP desconeguda (pot ser senyal de malware contactant un C&C).

    - Alerta de múltiples intents fallits de login d'un compte administrador o des de ubicacions geogràfiques atípiques.

    - Alerta si es desactiva inesperadament algun log o servei de seguretat (ja que un atacant podria intentar tapar rastres).

    - Alerta de pic de lectura de dades: p. ex., si de sobte es llegeixen milers de registres de la base de dades en poc temps fora de l'horari normal, indicador de possible **exfiltració**.

- Per implementar-ho, es faran servir tant les funcionalitats de **Cloud Monitoring (alertes sobre mètriques)** com de **Cloud Logging (alertes basades en patrons de logs)**. Aquestes eines permeten definir condicions i enviar notificacions. L'equip

de seguretat rebrà aquestes alertes via email i també a un canal dedicat (per exemple, un canal de Missatgeria o PagerDuty) segons la criticitat. Google Cloud ofereix a més serveis com **Security Command Center (SCC)** que agreguen deteccions de diverses fonts (inclosos patrons de comportament anòmal i anàlisi de vulnerabilitats) – EduTech habilitarà SCC en mode estàndard per rebre alertes de serveis com **Event Threat Detection** (que pot identificar activitat de malware coneguda a partir dels logs) o **Container Threat Detection** (si utilitzem Kubernetes, per detectar anomalies als containers).

- **Equip de resposta a incidents en entorn cloud:** El pla de resposta a incidents definit a la Pràctica 2 establia un equip i procediments generals. Ara, s'adaptarà aquest pla al context cloud. L'**Equip de Resposta a Incidents de Seguretat (CSIRT)** d'EduTech haurà d'estar preparat amb coneixements d'eines GCP. S'establiran rols clarament definits per incidents cloud, per exemple: un *Analista de Seguretat Nivell 1* que fa triatge d'alertes al SCC i Cloud Logging, un *Enginyer Cloud* que pot intervenir sobre les instàncies (per exemple, aïllar una VM compromesa), i un *Responsable de Comunicació* que en cas d'incident greu pugui informar la direcció i, si cal, usuaris afectats. El pla haurà de contemplar **escenaris específics**: què fer si es detecta un comportament indicatiu de ransomware en una VM (possiblement apagar l'instància i arrencar des d'un snapshot net), què fer si un bucket de dades ha estat exposat (tancar l'accés, analitzar logs per veure qui hi ha accedit), o com respondre si hi ha un ús indegut de claus d'API (revocar claus i rotar-les immediatament). Tots aquests procediments d'actuació estaran documentats i provats en simulacres periòdics.

- **Eines forenses i de contenció al núvol:** En cas d'incident, és important poder analitzar i contenir sense destruir evidències. EduTech aprofitarà funcionalitats de GCP per fer **forense digital al núvol**: per exemple, en detectar una instància compromesa, en lloc de apagar-la directament es podria fer un **snapshot del disc** per preservació d'evidència i després aïllar-la de la xarxa (canviant les regles de firewall) per investigar. Google Cloud permet clonar discos i adjuntar-los a màquines d'anàlisi per examinar fitxers maliciosos sense risc. També es poden utilitzar serveis com **Cloud IDS (Intrusion Detection System)** per inspeccionar el trànsit de xarxa en temps real durant l'investigació, o les eines de **Packet Mirroring** per capturar trànsit específic d'una VM sospitosa cap a un analitzador. La contenció ràpida es pot fer aprofitant l'elasticitat del cloud: per exemple, si una aplicació és atacada, es pot desplegar ràpidament un entorn alternatiu actualitzat mentre es retira el compromès. Tot això forma part de la capacitat de resposta dinàmica que el núvol facilita.

- **Integració amb SIEM corporatiu:** Si bé Cloud Logging i SCC cobreixen molt de l'entorn GCP, EduTech pot integrar aquestes fonts en un **SIEM** centralitzat que recopili logs de tota l'organització (incloent potser sistemes no-cloud o SaaS externs). En aquest cas, es crearien *exportacions de logs (log sinks)* per enviar els logs de seguretat de GCP cap al SIEM existent (per exemple, si es disposa d'una plataforma com Splunk, Elastic Security o Chronicle). Això permetria als analistes veure els incidents en el context més ampli i correlacionar, per exemple, un

esdeveniment al núvol amb un de la xarxa interna. Tot i no ser imprescindible si SCC està configurat, és una opció a considerar en l'estratègia global de monitorització.

- **Millora contínua i *post-mortem* d'incidents:** Després de cada incident o simulacre, es durà a terme un anàlisi *post-mortem* detallat, tal com s'indicava en el pla de resposta a incidents general. En context cloud, això inclou revisar si les alertes van saltar adequadament, si els responsables tenien les eines i permisos necessaris (per exemple, l'Enginyer Cloud tenia accés immediat per pausar una màquina), i quines mesures preventives noves es podrien implementar per evitar casos similars. Sovint, d'un incident s'aprèn i es decideix afegir una nova regla de detecció o ajustar una política. EduTech institucionalitzarà reunions post-incidents on es decidiran accions de millora (p. ex., arran d'un incident de phishing que va comprometre un compte, es podria decidir reforçar la formació als usuaris en aquest aspecte, a més de la resposta tècnica).

Amb tots aquests elements definits, és fonamental també establir un marc normatiu intern que enmarqui i doni coherència a l'estratègia: això es plasma en la **política bàsica de seguretat al núvol** que es presenta a continuació.

# Política Bàsica de Seguretat al Núvol

La política de seguretat al núvol és el document que recull de forma clara els **principis, normes i procediments** que EduTech Global adopta per protegir els seus actius al núvol. Mentre que l'estratègia defineix què s'ha de fer i com (mesures tècniques i operatives), la **política** estableix sobretot el marc de responsabilitats – és a dir, *qui* ha de fer què, *quan* i *des d'on*, per mantenir la seguretat, per tant, els principals punts de la política bàsica de seguretat al núvol d'EduTech són:

- **Abast i aplicació:** Aquesta política s'aplica a tots els sistemes i dades d'EduTech Global allotjats en serveis de computació al núvol (actualment, Google Cloud) així com als usuaris, empleats o col·laboradors que hi tinguin accés. Qualsevol ús de recursos cloud fora d'aquestes directrius queda prohibit sense aprovació expressa de l'equip de seguretat. La política és d'acompliment obligatori i el seu incompliment pot comportar mesures disciplinàries.

- **Responsabilitats clau:** Es designa formalment un **Responsable de Seguretat Cloud** dins l'equip de TI, encarregat de vetllar pel compliment d'aquesta política i d'actualitzar-la segons calgui. També es defineixen els **propietaris dels actius** cloud (per exemple, el cap de desenvolupament és propietari del servidor d'aplicacions, el cap de dades és responsable de la base de dades) que han d'assegurar que els seus respectius recursos compleixen les mesures de seguretat i informar de qualsevol canvi d'entorn. L'equip de seguretat és responsable de monitoritzar i auditar regularment els sistemes, mentre que tots els usuaris amb accés tenen la responsabilitat de seguir les pràctiques segures (com mantenir credencials confidencials, utilitzar MFA, etc.).

- **Gestió d'identitats i accessos:** Només els usuaris **autoritzats** poden accedir als recursos al núvol d'EduTech, i només en la mesura dels permisos atorgats pel seu rol. Totes les altes de nous usuaris o modificacions de permisos han de seguir un procés d'aprovació formal (sol·licitud, revisió per part de seguretat i autorització per un supervisor). És obligatori que **cada compte d'usuari sigui individual** (no es permeten comptes compartits) i que estigui vinculat a una persona o funció concreta. Tots els accessos administratius al cloud (consola GCP, accés a bases de dades, etc.) requeriran autenticació multifactor. Igualment, l'ús de comptes de servei ha d'estar justificat i documentat, i les claus d'aquests comptes, si s'utilitzen, han de ser gestionades de manera segura (registrades i rotades regularment). Cap usuari ha de tenir més permisos dels necessaris: s'implementa i es fa complir el **principi de privilegi mínim** en tot moment.

- **Control de xarxa i ubicació d'accés:** Les accions administratives crítiques (p. ex. desplegar nova infraestructura, canviar configuracions de seguretat, accedir a dades sensibles) s'hauran de realitzar des de la xarxa corporativa d'EduTech o mitjançant els mecanismes segurs aprovats (VPN corporativa o IAP de Google). L'accés directe des d'internet a les consoles d'administració queda desautoritzat, excepte si s'empra MFA i es justifica per necessitat urgent fora de l'oficina. A més, es recomana que

l'accés fora d'hores de feina a entorns de producció es limiti al personal de guàrdia i s'enregistri degudament. Aquest punt assegura el *"des d'on"* de l'accés: preferentment des d'entorns controlats.

- **Protecció de dades i classificació:** Totes les dades allotjades al núvol han de tenir una classificació assignada segons la seva sensibilitat (confidencial, interna, pública). Segons la classificació, s'aplicaran controls adequats: per exemple, dades classificades com a *confidencials* s'han de xifrar amb claus gestionades per EduTech (CMEK) i només ser accessibles per personal autoritzat de nivell alt; aquestes dades no es poden copiar a dispositius personals ni enviar fora dels sistemes corporatius sense autorització. Està estrictament prohibit emmagatzemar dades personals sensibles en serveis cloud externs o comptes no aprovats (com ara comptes personals de Google Drive, etc.). Les còpies de seguretat de dades crítiques s'han de fer regularment i emmagatzemar en ubicacions segures, complint els periodes de retenció definits. La política també obliga a complir les lleis de protecció de dades: p. ex., si es tracten dades de ciutadans europeus, aquestes s'han de mantenir en centres de dades de la UE o sota acords legals vàlids, i qualsevol incident de seguretat que afecti dades personals es notificarà conforme al pla de resposta i a la normativa (breach notification).

- **Seguretat de la infraestructura i canvis:** Qualsevol desplegament de nova infraestructura cloud (màquines, bases de dades, xarxes) ha de seguir els estàndards de configuració segura definits per l'empresa. S'utilitzarà preferentment **infraestructura com a codi** i plantilles aprovades per assegurar coherència. Abans de posar un nou servei en producció, l'equip de seguretat ha de realitzar un **anàlisi de riscos i prova de vulnerabilitats** sobre aquest (incloent, si escau, un pentest o revisió de configuració). Els **canvis significatius** en la configuració de seguretat (com ara regles de firewall, polítiques IAM crítiques, o paràmetres de xifrat) han de passar per un procés de gestió de canvis formal, incloent revisió per parells i documentació. Cap servidor o servei no monitoritzat ha d'executar-se en l'entorn cloud de producció: si es detecta un recurs sense els agents de monitorització o sense els logs activats, se li aplicarà quarantena fins que compleixi els requisits.

- **Monitorització i resposta a incidents:** Tal com recullen els procediments del pla de resposta a incidents, tots els esdeveniments de seguretat detectats han de ser notificats immediatament a l'equip de seguretat. Aquesta política estableix que la monitorització de seguretat és contínua i que les alertes crítiques (p. ex. intrusions confirmades, filtració de dades) han de desencadenar una resposta en menys d'un temps determinat (p. ex. 1 hora per alertes greus). El personal ha de conèixer els canals de comunicació en cas d'incident (a qui trucar, on està el runbook). També indica que després de qualsevol incident s'ha d'elaborar un informe d'incident i revisar les polítiques o mesures per evitar la recurrència. Complementàriament, es realitzaran **formacions periòdiques** als empleats en matèria de seguretat cloud, per assegurar que estan al dia en procediments (per exemple, com reconèixer un correu de phishing que busqui credencials GCP, o com reaccionar si es veu informació

sensible en un canal inadequat).

- **Compliment i auditories:** Per assegurar el compliment d'aquesta política, es duen a terme **auditories internes anuals** de la configuració i pràctiques de seguretat al núvol. A més, es podria sotmetre l'entorn a auditories externes o certificacions (com ISO 27001 o conformitat amb ENS si fos aplicable, etc.) per donar fe de la robustesa de la seguretat. Qualsevol desviació o no-conformitat detectada ha de ser corregida en un pla d'acció amb terminis definits. La direcció s'informarà periòdicament de l'estat de la seguretat al núvol i del grau de compliment de la política.

Aquesta política bàsica serà distribuïda a tots els equips relacionats i estarà disponible en el repositori de polítiques corporatives. És un document viu que es revisarà i actualitzarà a mesura que l'entorn cloud evolucioni, que apareguin noves amenaces o que l'empresa incorpori nous serveis. L'objectiu final és crear una **cultura de seguretat al núvol** dins EduTech Global, on cada membre comprengui la importància de seguir els procediments i on la tecnologia de seguretat sigui recolzada per normes clares.

# Conclusions

Amb la definició d'aquesta Estratègia de Ciberseguretat al Núvol, EduTech Global fa un pas endavant en la seva evolució cap a una infraestructura moderna i segura. Al llarg del document s'ha tractat **com protegir els actius cloud de l'empresa** des de múltiples angles: identificant els recursos crítics (servidors, dades, xarxes) i els riscos associats; establint controls d'accés robustos mitjançant IAM i principis de privilegi mínim; assegurant la confidencialitat i disponibilitat de les dades amb xifratge i còpies de seguretat; fortificant la infraestructura amb segmentació, firewalls i actualitzacions; i preparant la detecció i resposta eficient davant incidents amb eines avançades de monitorització i un equip capacitat. Tot això queda emmarcat dins una política bàsica que guia el *qui*, *quan* i *com* de la seguretat al núvol.

En coherència amb les pràctiques anteriors, EduTech Global consolida una **narrativa de millora contínua en ciberseguretat**: primer es van posar els fonaments (controls d'accés i arquitectura segura), després es va establir la vigilància i capacitat de resposta, i ara s'integra la seguretat en el seu futur ecosistema cloud. Implementant aquesta estratègia, l'empresa podrà migrar serveis al núvol amb garanties, aprofitant els avantatges de flexibilitat i escalabilitat sense comprometre la seguretat ni la privacitat dels seus usuaris.

Cal esperar que l'amenaça segueixi evolucionant; per tant EduTech Global mantindrà una actitud proactiva, revisant regularment l'eficàcia de les mesures proposades, adaptant-se a noves eines de Google Cloud i seguint les millors pràctiques del sector. El compromís de la direcció i de tota l'organització en el compliment de la política de seguretat al núvol serà clau per a l'èxit. En definitiva, amb aquesta estratègia, EduTech Global està preparada per afrontar els reptes de seguretat en la seva transformació digital cap al núvol, garantint la confiança dels seus usuaris i la continuïtat del negoci en tot moment. En endavant, qualsevol ampliació de l'ús del cloud anirà acompanyada de l'anàlisi de riscos corresponent i de l'enfortiment de les mesures aquí descrites, assegurant que la seguretat segueix sent un pilar fonamental del creixement tecnològic de l'empresa.

# Bibliografia


Google Cloud. (2023). *Security foundations guide*. Retrieved from https://cloud.google.com/security-foundations

Google Cloud. (2023). *Google Cloud Architecture Framework: Security*. Retrieved from https://cloud.google.com/architecture/framework/security

Google Cloud. (2023). *Cloud Identity and Access Management documentation*. Retrieved from https://cloud.google.com/iam/docs

Google Cloud. (2023). *Cloud Audit Logs documentation*. Retrieved from https://cloud.google.com/logging/docs/audit

Google Cloud. (2023). *Data Loss Prevention overview*. Retrieved from https://cloud.google.com/dlp/docs/overview

ENISA (European Union Agency for Cybersecurity). (2021). *Cloud Security for SMEs*. Retrieved from https://www.enisa.europa.eu/publications/cloud-security-for-smes

CIS (Center for Internet Security). (2023). *CIS Google Cloud Platform Foundation Benchmark v2.0.0*. Retrieved from https://www.cisecurity.org/benchmark/google_cloud_platform

OWASP Foundation. (2021). *OWASP Top Ten Web Application Security Risks*. Retrieved from https://owasp.org/www-project-top-ten/