Assaig i Presentació (AiP)

Seguretat i Privacitat

CPD

Efrén Carles Ramon i Karol Djanashvili
Q2 2021-2022

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Índex

1. Introducció

És ben sabut que des de fa uns anys la quantitat de dades a tractar i emmagatzemar d'empreses, organitzacions i altres s'ha incrementat com mai abans i és que ens trobem en l'era de la informació i aquesta, és molt preuada per a tots avui dia. Amb les necessitats sorgeixen solucions i no sorprèn que enormes companyies tecnològiques com Google, Microsoft o Amazon ofereix als usuaris plans per emmagatzemar i analitzar les seves dades, infraestructures de seguretat i privacitat entre altres de les seves moltes capacitats.

Avui dia la major part de les persones amb accés a Internet no acostumen a preocupar sobre on són emmagatzemant les seves dades o què s'està fent amb les seves dades sense el seu consentiment conscient. Aquest fet porta a la taula un dels temes més importants de la dècada, la seguretat i privacitat de les nostres dades.

Les empreses proveïdores de tecnologia com les esmentades anteriorment tenen un ampli nombre de serveis que faciliten la vida a grans empreses de tots els sectors i nínxols imaginables. És per això que creiem molt important saber de quina manera emmagatzemen les dades, com asseguren la disponibilitat d'aquestes dades en qualsevol moment, com protegiran les nostres dades contra indesitjables i de quina manera la llei regula aquestes situacions per protegir al client en contractar els serveis. En aquest treball parlarem sobre el tema en profunditat on resoldrem aquestes qüestions.

1.1 Breu Resum

Amazon

Amazon és una empresa que es va crear el 1994 per Jeff Bezos com una plataforma per a la venda de llibres a través d'Internet. Des de llavors els productes oferts per la companyia han incrementat i amb això els seus ingressos i la seva popularitat.

Amazon és coneguda avui dia com l'empresa de comerç electrònic més gran de món i també és el primer proveïdor de serveis al núvol per a les empreses a través d'Amazon Web Services.

Google

Google és una empresa que es va crear com un projecte universitari el 1996 per Larry Page i Sergey Brin. La idea era crear una plataforma per organitzar tota la informació disponible a la World Wide Web.

A poc a poc Google ha anat creixent mitjançant la creació de nous serveis com Google Maps, Google Docs, Google Cloud Platform etc. i la compra de companyies. Google té a la seva disposició milers de centres de dades a tot el món.

Microsoft

Microsoft es va fundar el 1975 per Bill Gates i Paul Allen. Microsoft es dedica a el desenvolupament, fabricació i producció de programari i maquinari electrònic entre altres coses. Entre els productes i serveis que ofereix trobem Windows, Azure, Office, Microsoft Edge, servidors web, Onedrive etc.

1.2 Què entenem per seguretat?

La seguretat de les dades és la pràctica de protegir la informació digital de possibles corrupcions, robatoris, errors o accessos no autoritzats. Això s'aplica a tots els aspectes que formen part de l'emmagatzematge i ús de dades, és a dir, des de la part de seguretat física com a la part de programari. La seguretat de les dades si s'implementa i compleix amb la seva comesa, proporcionés protecció a l'empresa contra ciber crims, errors humans etc.

A més, considerem que per tenir una seguretat de les dades és igual d'important la consciència que fa servir els serveis com de l'empresa que proveeix d'aquests.

2. Seguretat perimetral

La seguretat física de les instal·lacions és potser una de les més obviades per tots, ja que quan parlem de “seguretat informàtica” el que primer ens ve a la ment és “firewall” o “encriptació”.

Però protegir les instal·lacions on tenim el nostre CPD és una feina tan difícil com necessària. Necessites trobar un equilibri entre la seguretat del hardware i la conveniència dels operaris de les instal·lacions.

AWS - Amazon Web Services

Amazon implementa tot un seguit de polítiques que el que fan essencialment es controlar qui entra i surt de les instal·lacions a la vegada que es controla l’estat dels visitants que ja hi són a dintre:

En principi només es permet l'accés a les instal·lacions als treballadors de les mateixes i al personal de seguretat. Si una persona externa vol entrar-hi i té un motiu empresarial justificat, aquesta ha de fer una petició pels canals corresponents, la qual serà avaluada per personal especialitzat. Un cop aprovada, se li concedirà una targeta d'accés de visitant; els guàrdies de

seguretat tenen com a ordres el només deixar passar a les persones que vagin correctament identificades.

Quan ja sigui a dintre, el visitant es veurà monitorat constantment des d'una sala de monitoratge amb càmeres, alarmes a les portes i sensors de moviment i temperatura. Aquesta sala de monitoratge també s'encarrega de vigilar altres paràmetres que poden afectar el funcionament del centre de processament de dades, com per exemple la temperatura i humitat del centre.

En quant el visitant acabi la visita i surti de les instal·lacions els permisos li seran revocats automàticament.

Google Cloud

La seguretat a les instal·lacions de Google Cloud es basa en el que ells anomenen seguretat de 6 capes. 6 conjunts de mesures de seguretat de naturaleses diferents ens asseguren que els centres de processament de dades estan segurs:

1. **Capa 1:** La capa 1 és la més simple, tot un seguit de valles i senyals cobreixen el perímetre de la propietat on està construït el CPD.

2. **Capa 2**: La capa dos és on les coses es comencen a posar interessants, aquesta consta de valles intel·ligents que detecten si algú les està tocant, guàrdies que patrullen 24/7, càmeres amb visió tèrmica i aparells de seguretat que poden aturar fins a un camió amb el remolc ple.

3. **Capa 3:** la capa 3 és la que s'encarrega de gestionar l'accés als edificis. Cada visitant ha de portar a sobre una targeta identificadora que se li proporciona abans d'entrar a les instal·lacions una vegada s'ha identificat. No només es verifica que té una targeta d'identificació sinó també se li fa una anàlisi ocular per a assegurar-se que la persona és realment qui diu a la identificació.

4. **Capa 4:** la capa 4 es la capa que se'n encarrega de monitoritzar tot el CPD els 365 dies de l'any, les portes, les càmeres, escáner ocular, etc. Tot està connectat a aquesta capa.

5. **Capa 5:** Aquesta és la capa que garanteix l'accés als dispositius físics, és una capa on només hi tenen accés les persones que realment necessiten tenir-lo: tècnics i enginyers que mantenen i/o milloren la infraestructura.

   Encara que Google tingui accés als dispositius físics, els clients poden establir la seva pròpia encriptació de claus privades, així que l'empresa no té accés a les dades dels dispositius.

6. **Capa 6:** Aquesta és l'última capa i és la que garanteix que dels residus que genera el centre de processament de dades no se'n pot extreure informació, destruint i reciclant correctament els discs durs i les màquines que ja no es poden fer servir.

Azure

Microsoft Azure segueix el mateix principi que Amazon a l'hora de gestionar la seguretat dels seus datacenters, un control exhaustiu de les persones que hi accedeixen:

- Petició d'accés: Totes les persones que vulguin accedir a les instal·lacions hauran de passar per un procés de petició, justificant una raó vàlida per fer-ho. Aquesta petició serà avaluada per un equip de persones que comprovaran les dades proporcionades pel visitant.

  Si la petició acaba sent aprovada el permís que se li concebrà només li permetrà accedir a les parts del CPD estrictament necessàries i durant un període limitat de temps.

- Perímetre de les instal·lacions: Per accedir a l'interior del CPD és necessari passar per un únic punt d'accés amb control de detector de metalls, càmeres i guàrdies de seguretat.

- Entrada a l'edifici: L'entrada a l'edifici està plena de guàrdies de seguretat i personal de la instal·lació a qui se'ls ha entrenat rigorosament.

- Interior del centre: Un cop a dintre del centre, has de passar 2FA amb biometria per a accedir a la part del CPD on se't permet accedir, i només pel temps que se t'ha concedit.

- Datacenter: Només es permet accedir a aquest nivell si és estrictament necessari i després de passar per un escàner de detecció de metalls; també és necessari que el visitant deixi totes les motxilles o bosses que pugui portar a l'entrada.
  Serà necessari que faci el mateix procediment a la sortida, passant pel detector de metalls. Podrà recuperar les bosses quan surti de les instal·lacions.

3. Seguretat en la infraestructura

Les mesures de seguretat que protegeixen la infraestructura tenen com a prioritat protegir la integritat física del hardware que conté el CPD, ja siguin els servidors, els discs i altres aparells que conformen el centre.

AWS - Amazon Web Services

Una de les característiques d'aquest nivell de protecció són els mantraps, portes giratòries que mai deixen una via d'accés directe. Un cop la persona ha entrat dins, la càpsula es tanca, deixant a la persona atrapada dins (d'aquí el nom) i quan l'accés està tancat s'obre la sortida. Aquest mecanisme per entrar dins l'edifici ofereix control total a AWS i a més fa que les persones entrin d' 1 en 1 i no entrin amb grups, possiblement aprofitant la confusió de l'aglomeració per saltar-se les mesures de seguretat.

Diagnòstics rutinaris de les màquines, les xarxes de comunicació i dels equips complementaris (NAS, SAI, etc) són realitzats periòdicament per a assegurar que tot funciona sense problemes. En tots els sistemes d'alimentació i xarxa existeix redundància N +1, també s'ofereix un pla de contingència en cas de desastre natural que fa ús de nombrosos sensors per detectar-los i posar en marxa equips de resposta.

Així i tot, la ubicació és un factor molt important a considerar quan es decideix on construir el CPD i també es té en compte si el terreny on es construeix té algun risc especialment alt de terratrèmols, inundacions, incendis o tornados.

Google Cloud

De forma semblant a AWS Google Cloud també implementa mesures de seguretat de forma molt estricta pel que fa a l'accés al seu hardware. Només els enginyers i tècnics del CPD tenen accés a la part de les instal·lacions que emmagatzema el hardware. Si es vol accedir s'ha de passar per un seguit de controls d'accés, tan de biometria com escorcolls físics, detectors de metall i varies proves més.

Cada rack està vigilat com si fos una caixa forta, amb càmeres que apuntant a la part frontal i posterior de l'armari. No es permet entrar ni treure cap dispositiu electrònic no comprovat de les instal·lacions, per a evitar possibles robatoris de discs o d'altres aparells.
Pel que fa a la seguretat que protegeix el CPD de desastres naturals, tots els centres compten amb un sistema d'extinció d'incendis per extracció d'oxigen, aquest no deixa residus i no afecta el hardware a diferència dels sistemes convencionals d'aigua.
Altres sistemes com portes automàtiques, alarmes i diversos mecanismes de control d'accés són controlats des d'una sala de control central que monitora tot l'edifici.

Azure

Seguint el mateix camí que AWS i GC, Azure es prepara perquè els seus CDPs puguin resistir un desastre natural.
Les fonts d'alimentació ininterrompudes i els grans bancs de bateries garanteixen que l'electricitat continuï si es produeix una interrupció de l'energia a curt termini. Els generadors d'emergència proporcionen energia de seguretat per a interrupcions prolongades i manteniment previst. Si es produeix un desastre natural, el centre de dades pot utilitzar reserves de combustible in situ.

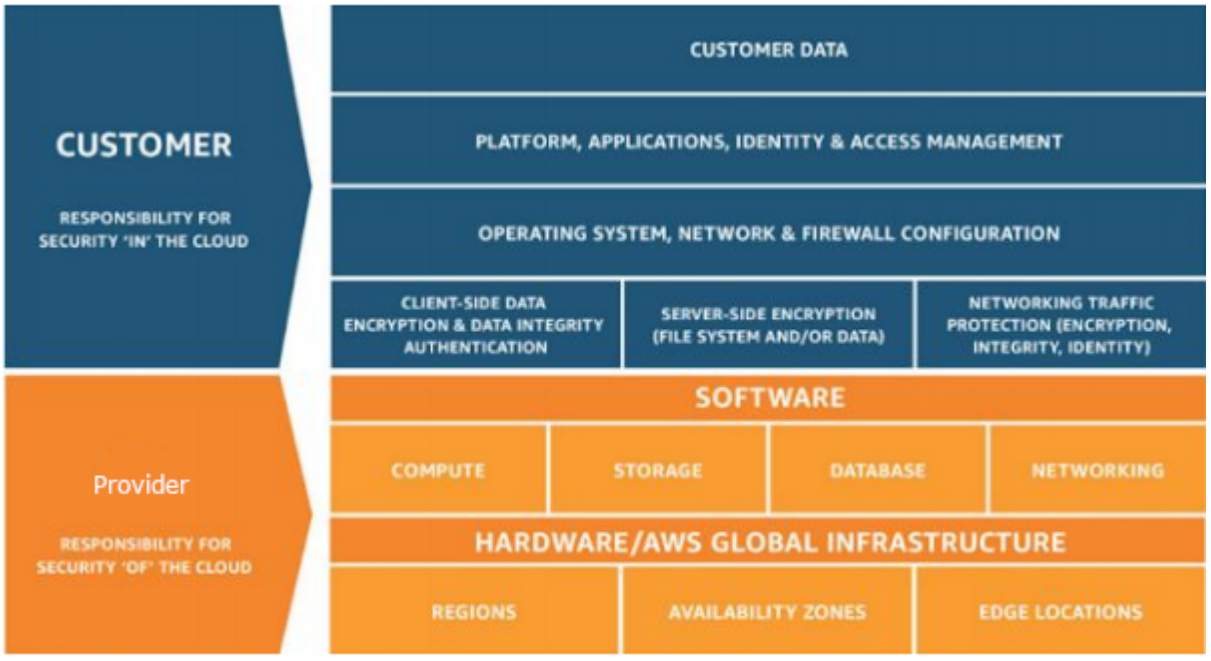
4. Integritat de dades

Una de les parts més importants pel que fa a la seguretat d'un CDP és la integritat de les dades, podem garantir que unes dades són privades i que ningú hi accedeix, però no ens serveix de res si aquestes dades deixen d'existir o si poden ser accedides per la mateixa empresa que ens hosteja els serveis.

En aquest apartat no només veurem com les empreses de host protegeixen i garanteixen la disponibilitat de les nostres dades sinó a més, com garanteixen privacitat inclús dintre de la seva pròpia empresa.

Així i tot, també veurem que en el món del Cloud la seguretat de les dades no només és responsabilitat dels proveïdors sinó que més aviat segueix un model de responsabilitat compartida.

Sí que és cert que cada proveïdor ha de garantir la seguretat lògica i física de la infraestructura, però el que es faci amb la infraestructura proveïda és responsabilitat del client. Si instal·la software maliciós, filtra les credencials o no actualitza les tecnologies utilitzades a versions més noves amb possibles millores de seguretat serà responsabilitat només del client.



AWS - Amazon Web Services

Suposem que un intrús ha aconseguit l'impossible, ha accedit a la sala de servidors i està intentant esborrar o modificar les dades d'una de les màquines, aquestes estan programades per a apagar-se automàticament i notificar a la sala de control si hi ha hagut un accés no autoritzat.

No fa falta dir que ja es compten amb firewalls, load balancers, virtualització, honey pots i mil mecanismes de seguretat mes per a garantir la seguretat de les dades dels clients envers un atac informàtic.

No només a atacs realitzats des de fora sinó també atacs realitzats des de dintre, la tecnologia de la virtualització permet a dos clients compartir la mateixa màquina sense poder accedir l'un als recursos de l'altre.

Per a facilitar que els usuaris tinguin un entorn segur, l'agost de 2016 Amazon va publicar un document de 74 pàgines detallant les millors pràctiques. A més, ofereixen un seguit d'eines de seguretat per tal d'implementar les pràctiques esmentades, com CloudTrail, AWS WAF, Amazon Inspector o Cloud Front.

Google Cloud

Totes les dades dels clients dintre del Google Cloud estan encriptades, tant les dades que es troben en trànsit (comunicacions i/o dades sent usades per les màquines) com les dades en repòs (dades a disc, sense ser utilitzades). Inclús les claus d'encriptació d'aquestes dades estan encriptades utilitzant una clau d'encriptació de claus (KEK). Aquest concepte es coneix com a encriptació envelope.

Cada operació de dades inclou una comprovació de corrupció de dades. Si es detecten errors l'operació s'anul·la i s'enregistra l'error. Aquestes comprovacions es realitzen comprovant els checksums dels operands.

Azure

Azure ofereix un servei de bases de dades conegut com AzureSQL i gran part dels seus mitjans de protecció de dades són dedicats a la protecció d'aquestes bases de dades.

Primerament, AzureSQL alera els seus usuaris quan es troba una excepció no tractada, cosa que pot significar que existeix corrupció de dades.
La creació i restauració en cas de fallada de backups està completament automatitzada.

Una de les causes més comunes a l'hora de parlar de corrupció de dades en bases de dades són els anomenats "lost writes". Identificant cada operació amb un identificador podem observar si hi ha hagut alguna operació que ha fallat i que per tant no s'ha registrat, veien un salt a les ID's consecutives de les operacions.

5. Auditories

Les auditories de seguretat permeten avaluar el nivell de seguretat que té l'organització, és a dir, una auditoria s'encarrega d'analitzar les polítiques, procediments, actuacions definits per una empresa per revisar tant el nivell de compliment que tenen d'aquestes.

Les auditories poden estar realitzades per tercers (auditoria externa) que serien persones o companyies externes que analitzen debilitats o/i vulnerabilitats en el cicle de seguretat de l'empresa. També és possible que l'organització tingui un equip dedicat a la cerca de riscos dins l'empresa, això es coneix com una auditoria interna.

La majoria de les auditories es fan per conèixer de quina manera un atacant, lladre o qualsevol usuari amb objectius maliciosos podria explotar la seguretat de l'organització que poden ocasionar grans pèrdues econòmiques entre d'altres.

A continuació expliquem com fan auditories en els serveis d'Amazon Web Services, Google Cloud i Azure.

AWS - Amazon Web Services

Amazon es sotmet a auditories externes durant tot l'any de manera freqüent. A més a Amazon existeix l'equip de gestió de risc empresarial i observança (ERMC) que és una auditora interna responsable d'identificar els principals riscos que pot tenir l'organització. A més, certifica que el fet que es duen a terme les activitats apropiades definides per l'empresa en casos de risc.

Dins de l'equip ERMC, també tracten les auditories i un dels objectius és el de mitigar els riscos mitjançant l'ús de solucions tecnològiques i la metodologia de gestió. Els auditors busquen riscos que puguin perjudicar a l'empresa.

Segons les comprovacions de l'auditoria, sabem que els auditors poden fer el següent:

- Entrevistar als treballadors: Poden entrevistar als treballadors per verificar com fan ús del hardware o les instal·lacions.
- Revisar la videovigilància: Poden veure les gravacions fetes per les càmeres de seguretat a les instal·lacions (sales, habitacions, passadissos, etc.)
- Documentar les observacions que ha realitzat durant les auditories
- Examinar equips: examinar els equips de seguretat, logs (monitoratge), sensors, etc.

Google Cloud

Igual que AWS d'Amazon, Google Cloud es sotmet a auditories externes durant tot l'any de manera freqüent. Els auditors externs tenen accés diversos cops a l'any per revisar l'organització. Cal destacar que l'auditor no té autorització per visualitzar les dades als registres d'activitat d'administració de l'empresa.
Per complir aquest requisit, hi ha disponible un tauler que proporciona accés als registres històrics emmagatzemats a BigQuery i als registres d'activitat de l'administrador de Cloud Logging.
L'organització crea un grup de Google per a aquests auditors externs i afegeix l'auditor actual al grup. Aquest grup es controla i normalment se li concedeix accés quan és necessari. Al final de cada període d'auditoria, es revoca l'accés del grup.
Les dades es redacten mitjançant Cloud DLP abans de ser accessibles per visualitzar-les mitjançant l'aplicació del tauler de control.

Azure

L'auditoria Azure SOC 2 de tipus 2 es basa en els principis i criteris dels serveis de confiança de l'American Institute of Certified Public Accountants (AICPA), que inclouen seguretat, disponibilitat, confidencialitat, privadesa i integritat del processament, i els criteris de la Cloud Security Alliance (CSA) Matriu de controls de núvol (CCM).

Les certificacions Azure SOC 2 es basen en auditories independents i rigoroses fetes per tercers, més concretament fetes per una empresa de bona reputació.

Al finalitzar una auditoria SOC 2, l'auditor emet un document amb la seva opinió en un informe SOC 2 tipus 2, que descriu el sistema del proveïdor de serveis al núvol i avalua la justícia de la descripció que ha fet, avalua els controls, si funcionen en una data específica, si funcionen eficaçment, etc.

Els informes Azure SOC 2 tipus 2 són rellevants per a la seguretat del sistema, la disponibilitat, la integritat del processament de dades, la confidencialitat, etc.

6. Protecció de dades

Sabem, que tant AWS com Google Cloud com Azure fan el possible per emmagatzemar les dades de manera segura, respectant la privacitat. En aquest apartat analitzem què fa cadascuna d'elles amb les dades dels seus milers i milions de clients.

AWS - Amazon Web Services

Els clients són els propietaris del seu contingut. A més, pot seleccionar quins serveis de AWS poden processar, emmagatzemar i allotjar el seu contingut, també poden seleccionar el tipus d'emmagatzematge i la regió geogràfica on volen emmagatzemar-ho. Una de les coses a tenir en compte és que pot ser que no tots els serveis d'AWS estiguin disponibles a totes les regions d'AWS.

AWS constata clarament que no accedeixen al contingut del client ni el fan servir les dades per altre fi sense el seu consentiment. Deixen clar que no extreuen informació per a màrqueting o publicitat.

AWS permet al client triar l'estat de seguretat del seu contingut. Ofereixen als clients un xifrat segur al contingut en trànsit i en repòs i, ofereixen l'opció d'administrar les seves pròpies claus de xifrat.

Google Cloud

A Google Cloud existeixen els responsables del tractament de dades que, estan obligats, entre altres coses, a emprar únicament encarregats del tractament de dades que ofereixin garanties suficients per implementar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme amb els requisits del GDPR. A continuació analitzem alguns aspectes que et convé tenir en compte quan avaluïs els serveis de Google Workspace.

A Google Cloud, busquen prioritzar i millorar tant la seguretat com la privacitat de les dades personals dels clients. Diuen que els clients poden usar els serveis amb la tranquil·litat que es compleixen les mesures del GDPR.

Azure

Azure també segueix la normativa del GDPR per la protecció de dades dels clients que posen les seves dades en mans dels seus serveis.

La Política d'Azure permet definir polítiques en l'àmbit de l'organització per gestionar recursos, assegura que els clients tinguin les seves dades encriptades i es mantinguin en una regió específica per complir el GDPR.

7. Legalitat

En terminis de legalitat ens trobem amb moltes lleis vigents segons el país o continent en el qual es trobi l'empresa o els seus usuaris/clients una de les grans i conegudes lleis vigents avui dia, que de fet han tingut una gran repercussió en els últims 2-3 anys a causa del canvi que van suposar a gran part de les empreses amb usuaris europeus és la GDPR.

GDPR

Una d'aquestes és el reglament europeu conegut com a GDPR que està relacionat amb la protecció del tractament de les dades personals dels usuaris i la transmissió/circulació de les dades.

El GDPR va entrar en vigor el maig de 2016 i va ser aplicat finalment el maig de 2018. Aquest període de temps va permetre a moltes empreses i organitzacions adaptar-se a la normativa per poder complir-la correctament.

El que fa el GDPR defineix els requisits concrets que s'han de complir per part de totes les empreses i organitzacions que tinguin la seva seu a Europa o que donin serveis a usuaris de la Unió Europea dels quals tinguin o/i recopilin informació de caràcter personal del tipus que siguin. No és desconegut que les multes pel no compliment del GDPR poden arribar als 20 milions d'euros depenent de l'empresa o situació.

Regula com poden recollir, usar i emmagatzemar dades personals a les empreses.
Tant AWS d'Amazon, Google Cloud de Google i Azure de Microsoft compleixen i segueixen el GDPR al peu de la lletra.

8. Solucions alternatives

Els 3 proveïdors que hem mencionat són els més populars i dominants del mercat per un gran marge, però també hi ha proveïdors molt més petits que, en funció de les teves necessitats, poden representar una millor solució que els proveïdors més grans.

Per què voldria decantar-me per un proveïdor més petit?

- Millor relació amb els clients: Les empreses més grans solen tenir un sistema d'atenció al client molt més automatitzat i feixuc a causa del seu gran nombre de clients.

- Especialització: Empreses molt més grans com ara AWS acostumen a oferir "una mica de tot", això sol significar que les solucions que ofereix són genèriques. Una empresa més petita pot centrar el seu mercat en un conjunt de serveis més petit però especialitzat.

- Solucions a mida: Molts proveïdors més petits ofereixen solucions a mida per a cada un dels seus clients, òbviament a un preu.

Un exemple de proveïdors de Cloud menys coneguts són Cisco Cloud i DigitalOcean, sent DigitalOcean el més popular dels dos amb la seva solució basada en droplets.

Encara que DigitalOcean ofereix una completa personalització pel que fa a la seguretat de les màquines virtuals que ofereix els seus client, les mesures de seguretat que implementa als seus centres de processament de dades no estan tan bé documentades com altres proveïdors més famosos.

9. Conclusions

En resum, la seguretat al món del Cloud és un tema que els proveïdors de serveis es prenen molt seriosament. Encara que arriben a existir certes diferències en com cada proveïdor tracta i protegeix als seus usuaris, una de les bases comunes a tots els proveïdors.

Una possible reflexió és que molts dels usuaris del cloud no paren molta atenció a la seguretat de la seva infraestructura perquè creuen que amb les mesures que ja apliquen els proveïdors en tenen prou.

I sí, les mesures de seguretat que implementant tant Google cloud, com Microsoft Azure o AWS fan que els seus serveis siguin extremadament segurs, però això no treu la responsabilitat del client en verificar que les seves dades estiguin segures.

Totes les plataformes ofereixen la possibilitat de gestionar l'encriptació amb claus privades pròpies, cosa que tothom hauria de fer.

10. Referències

Introducció

- www.expansion.com/economia-digital/companias/2019/03/10/5c8292b7468aeb567d8b45ee.html

Auditories

- https://www.ccn.cni.es/index.php/es/ccn-cert-menu-es/vigilancia-de-seguridad/auditorias-de-seguridad
- https://www.grupomeridian.com/auditoria-seguridad-informatica/
- https://docs.aws.amazon.com/es_es/general/latest/gr/aws-security-audit-guide.html
- https://www.amazon.jobs/es/teams/audit
- https://aws.amazon.com/es/compliance/auditor-learning-path/
- https://cloud.google.com/iam/docs/job-functions/auditing

Protecció de dades

- https://aws.amazon.com/es/compliance/data-privacy-faq/
- https://cloud.google.com/security/gdpr?hl=es
- https://support.google.com/a/answer/2888485?hl=es#zippy=%2Cadenda-sobre-tratamiento-de-datos-dpa-o-versiones-posteriores

Seguretat perimetral

- https://cloud.google.com/security
- https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Seguretat de la infraestructura

- https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Integritat de les dades

- https://cloud.google.com/kms/docs/data-integrity-guidelines

Altres solucions

- https://metrixdata360.com/cloud-series/top-cloud-providers/

Legalitat

- https://www.tecnous.com/que-es-gdpr-y-por-que-debemos-tenerlo-en-cuenta/
- https://www.bbva.com/es/gdpr-nueva-ley-europea-proteccion-datos/
- https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf
- https://www.aepd.es/es

- https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es