Escola Tècnica Superior d'Enginyeria
Electrònica i Informàtica La Salle

Treball Final de Màster

Màster Universitari en Enginyeria de Telecomunicació

Anàlisi de la ciberseguretat en la migració cap a entorns cloud

Alumne

Laura Abellanet Molhoek

Professor Ponent

Júlia Sánchez Rodríguez

ACTA DE L'EXAMEN
DEL TREBALL FI DE CARRERA

Reunit el Tribunal qualificador en el dia de la data, l'alumne

D. **Laura Abellanet Molhoek**

va exposar el seu Treball de Fi de Carrera, el qual va tractar sobre el tema següent:

Anàlisi de la ciberseguretat en la migració cap a entorns cloud

Acabada l'exposició i contestades per part de l'alumne les objeccions formulades pels Srs. membres del tribunal, aquest valorà l'esmentat Treball amb la qualificació de

Barcelona,

VOCAL DEL TRIBUNAL VOCAL DEL TRIBUNAL

PRESIDENT DEL TRIBUNAL

"L'experiència no és allò que et passa, sinó el que fas amb el que et passa."

Huxley, A. (1932) [Text and Pretexts]

Resum

El món de la ciberseguretat està avançant de forma molt ràpida, i amb l'aplicació de la nova llei europea de protecció de dades (GDPR) i la irrupció del cloud computing com a eina per proporcionar serveis informàtics assegurant una reducció de costos per part de les empreses, sembla que el sector està realitzant una revisió de tot el que hi havia desplegat fins ara per assegurar que els clients segueixen estant coberts a nivell de seguretat de la informació amb els controls que tenen aplicats.

D'aquí va sorgir la meva motivació per fer aquest treball. El que em preguntava era: com podem garantir a un client que, amb la migració dels seus sistemes IT al cloud segueix cobert a nivell de seguretat? Apliquen els mateixos controls definits fins al moment o cal incorporar-ne de nous? Realment li suposa una avantatge aquesta migració?

L'objectiu principal del projecte, doncs, és analitzar la diferència de nivell de risc de seguretat al què està exposat una empresa del sector financer segons si utilitza una solució cloud o una solució on-premise per desplegar els diferents sistemes IT.

Per assolir l'objectiu, s'estudien els següents punts:

- Les diferents normatives relacionades amb la seguretat de la informació i la privacitat de les dades.
- Els principals òrgans de govern de la ciberseguretat (tant a nivell mundial com europeu com estatal).
- Les principals amenaces a tenir en compte (tant a nivell genèric com específiques per les solucions cloud computing).
- Els principals incidents de ciberseguretat i costos derivats.
- Els diferents marcs de control existents per a la mitigació de les amenaces identificades.

I es planteja la metodologia a seguir per tal de dur a terme l'anàlisi de riscos, que permetrà, en última instància, respondre les preguntes mencionades anteriorment.

El cas d'ús es planteja amb la migració del correu electrònic al cloud amb Office365 i s'avalua si existeixen les eines de seguretat necessàries per mitigar el risc afegit que suposa tenir els sistemes IT de correu electrònic al cloud. Per fer-ho, es realitza un estudi previ de la solució Office 365 i un anàlisi dels riscos tenint en compte diferents escenaris. A continuació, s'inclou una comparativa amb la mateixa solució implementada on-premise per extreure pros i contres de la migració a un sistema cloud.

Paraules clau

Ciberseguretat – Cloud computing – Office365 – Cloud Security Alliance – Principals amenaces ciberseguretat – anàlisi de riscos – marc de controls de seguretat

Resumen

El mundo de la ciberseguridad está avanzando muy rápidamente. Con la aplicación de la nueva ley europea de protección de datos (GDPR) y la irrupción del cloud computing como herramienta para proporcionar servicios informáticos asegurando la reducción de costes por parte de las empresas, parece que el sector está realizando una revisión de todo lo que tenía desplegado hasta el momento para asegurar que siguen estando cubiertas a nivel de seguridad de la información con los controles que tienen implementados.

Así surgió la motivación de realizar este trabajo. Mi pregunta era: ¿cómo podemos garantizar a un cliente que, con la migración de sus sistemas IT al cloud sigue cubierto a nivel de riesgos de seguridad? ¿Aplican los mismos controles definidos hasta el momento o se necesita incorporar controles nuevos? ¿Realmente supone una ventaja esta migración?

El objetivo principal del proyecto es analizar la diferencia a nivel de riesgo de seguridad al que se expone una entidad del sector financiero según si utiliza una solución cloud o una solución on-premise para desplegar los diferentes sistemas IT.

Para alcanzar el objetivo, se estudian los siguientes puntos:

- Las distintas normativas relacionadas con la seguridad de la información y la privacidad de los datos.
- Los principales órganos de gobierno de la ciberseguridad (tanto a nivel mundial, como europeo, como estatal)
- Las principales amenazas a tener en cuenta (tanto a nivel genérico como específicas de las soluciones cloud computing).
- Los principales incidentes de ciberseguridad y costes derivados.
- Los distintos marcos de control existentes para la mitigación de las amenazas identificadas.

Y se plantea la metodología a seguir para llevar a cabo el análisis de riesgos, que permitirá responder a las preguntas mencionadas anteriormente.

El caso de uso se plantea con la migración del correo electrónico al cloud con Office365 y evalúa si existen las herramientas de seguridad necesarias para mitigar el riesgo añadido que supone tener los sistemas IT al cloud. Para hacerlo, se realiza un estudio previo de la solución Office 365 y un análisis de riesgos teniendo en cuenta los posibles escenarios. A continuación, se incluye una comparativa con la misma solución implementada on-premise para extraer pros y contras de la migración a un sistema cloud.

Palabras clave

Ciberseguridad – Cloud computing – Office365 – Cloud Security Alliance – Principales amenazas ciberseguridad – análisis de riesgos – marco de controles de seguridad

Abstract

Cybersecurity world is growing exponentially. With the application of the new European Data Protection Law (GDPR) and the emergence of cloud computing as a tool to provide cheaper IT services solutions, the sector is reassessing all solutions deployed until today to ensure that they are still covered by the implemented information security controls.

That is how I found the motivation to carry out this work. The main question was: how can we guarantee a customer that, with the migration of their IT systems to the cloud they are still covered in terms of information security? Do the same controls defined so far apply or do we need to incorporate new ones? Is the migration to cloud really an advantage?

The main goal of the project, therefore, is to analyze the difference in terms of cybersecurity risk level to which an entity in the financial sector is exposed based on whether it uses a cloud solution or an on-premises one to deploy the different IT systems.

To reach the objective, the following points are studied:

- Different regulations related to information security and data privacy.
- Main cybersecurity governance bodies (both global and European).
- Main threats to be considered (both generic and specific to cloud computing solutions).
- Main incidents of cybersecurity and derived costs.
- Different existing control frameworks for the mitigation of identified threats.

Additionally, the methodology to be followed to carry out the risk analysis will be explained.

The proposed use case is the migration of email to cloud with Office365 and assesses whether the necessary security tools exist to mitigate the added risk posed by having IT systems migrated to the cloud. To do so, a preliminary study of the Office 365 solution and a risk analysis taking into account the possible scenarios is carried out. To end up, a comparison between the cloud solution and the same solution implemented on premise is carried out and conclusions on pros and cons of the migration to a cloud system are extracted.

Key words

Cybersecurity – Cloud computing – Office365 – Cloud Security Alliance – Cybersecurity main threats – Risk analysis – Security control framework

Agraïments

En primer lloc m'agradaria agrair aquest treball als meus pares. Pel vot de confiança donat, pels recordatoris espaiats però periòdics, per l'ajuda durant la realització del treball i sobretot per estar sempre al meu costat. De ben segur que no estaria on estic si no fos per ells.

I en segon lloc al meu company de treball, el Miquel. Per animar-me en una primera instància a tornar-m'hi a posar, per motivar-me al llarg de tot el procés i per ajudar-me sempre que ho he necessitat. Ha estat un plaer.

Índex

Índex d'il·lustracions

Índex de taules

Glossari

ACLs

(NIST, 2013) Registre:

- d'usuaris que se'ls hi ha donat permís per utilitzar un sistema concret.
- tipus de permisos que tenen assignats.

Amenaça interna

(ENISA, 2018) Atacs per part d'usuaris interns de l'organització que utilitzen el seu accés autoritzat per perjudicar la seguretat de l'empresa. Poden ser atacs deliberats o inconscients.

Anti-virus

(NIST, 2013) Programa que monitoritza un ordinador o una xarxa per identificar els principals tipus de malware i prevenir o contenir els possibles incidents derivats.

APIs (Application Programming Interface)

(Inc, Accessed 2018) Conjunt de protocols, rutines, funcions i/o comandes que utilitzen els programador per desenvolupar programari o facilitar la interacció entre diferents sistemes.

Back-up

(NIST, 2013) Còpia de fitxers i programes feta per facilitar la recuperació d'un sistema.

Blacklisting

(NIST, 2013) Procés d'un sistema per invalidar:

- l'identificador d'un usuari basat en accions inadequades d'aquest. Un usuari que es troba dins la llista negra no podrà ser utilitzat per entrar al sistema, tot i tenir un identificador vàlid.
- Direccions IP associades a activitats indegudes per prevenir un ús no autoritzat o inadequat dels recursos d'Internet.

Botnets

(ISACA, 2017) Terme derivat de xarxa robot és una xarxa automatitzada i distribuïda d'ordinador prèviament compromesos que pot ser controlada de forma simultània per llançar atacs a gran escala a les víctimes escollides (com ara atacs de denegació de serveis).

BYOD (Bring your own Device)

(ISACA, 2017) Ús dels dispositius mòbils privats per accedir i treballar amb la informació de l'organització per la qual l'usuari treballa.

Ciber-espionatge

(ISACA, 2017) Activitats realitzades en nom de seguretat, negoci, política o tecnologia per trobar informació que hauria d'esser mantinguda en secret.

Cross-site Scripting (XSS)

(NIST, 2013) Vulnerabilitat que permet als atacants injectar codi maliciós en una pàgina web inofensiva. Els scripts adquireixen permisos dels scripts generats per la pàgina web objectiu i poden comprometre la confidencialitat i integritat de les transferències de dades entre la pàgina web i el client. Les pàgines web són vulnerables

	si mostren informació al client en resposta a peticions o formularis que no han estat correctament programats i accepten executables.
Dark web	(Inc, Accessed 2018) Conjunt de pàgines web que són visibles al públic però les seves adreces IP s'amaguen de forma intencionada.
DDoS (Distributed Denial of Service)	(NIST, 2013) Tècnica de denegació de servei que utilitza nombrosos hosts per realitzar l'atac.
DLP (Data Loss Prevention)	(ISACA, 2017) Programari que permet la detecció i prevenció de la fuga d'informació d'una organització.
Doble factor d'autenticació	(ISACA, 2017) Combinació de més d'un mètode d'autenticació com ara token i contrasenya o token i dispositiu biomètric.
Dos (Denial of Service) o PDoS (Permanent Denial of Service)	(ISACA, 2017) Atac a un servei des d'una font que l'inunda a peticions fins a desbordar-lo de tal forma que o atura completament el sistema o aquest opera a un ritme significativament menor.
Dumpster diving	(Inc, Accessed 2018) Ús de diversos mètodes per obtenir informació sobre un usuari, fonamentalment mètodes físics.
Encriptació	(NIST, 2013) Convertir el text pla amb text xifrat mitjançant un algoritme d'encriptació.
Enginyeria social	(NIST, 2013) Intent d'enganyar a una persona perquè desveli informació que pot ser utilitzada per atacar sistemes o xarxes (p.e. contrasenyes).
Exploit Kits	(Trendmicro, 2018) Tipus d'instrument utilitzat pels ciber criminals per explotar les vulnerabilitats dels sistemes i distribuir malware o realitzar altres accions malicioses.
Filtració de dades	(ENISA, 2018) Exposició voluntària de dades confidencials, sensibles o de propietat.
Firewall	(NIST, 2013) Gateway que limita l'accés entre xarxes conforme les polítiques locals de seguretat.
Fuga d'informació	(NIST, 2013) Exposició voluntària o no de dades confidencials, sensibles o de propietat.
Gateways	(NIST, 2013) Interfície que proporciona compatibilitat entre les xarxes adaptant les velocitats de transmissió, protocols, codis o les mesures de seguretat.
GDPR (General Data Protection Regulation)	(Union, 2018) Reglament europeu mitjançant el qual l'Eurocambra, el Consell de la Unió Europea i la comissió europea volen enfortir i unificar la protecció de dades per tots els països de la UE, controlant també la transferència de dades fora de la unió.
Hacker	(ISACA, 2017) Una persona que intenta aconseguir accés no autoritzat a sistemes informàtics.

Hashing	(NIST, 2013) Procés d'utilitzar un algoritme matemàtic sobre les dades per produir un valor numèric que és representatiu de la data.
IDMS (Integrated Database Management System)	(Inc, Accessed 2018) Model de gestió de bases de dades per mainframes.
AI (Artificial Intelligence)	(Inc, Accessed 2018) Àrea que es dedica a la creació de màquines intel·ligents que funcionen i reaccionen com humans. Algunes funcions inclouen: reconeixement de la parla, aprenentatge, planificació, solució de problemes.
IoT (Internet of Things)	(ISACA, 2017) Objectes físics que han integrat elements de xarxa i informàtics que els permet comunicar-se amb altres objectes mitjançant una xarxa (normalment, mitjançant internet).
IPS (Intrusion Prevention System)	(NIST, 2013) Sistemes que poden detectar activitat intrusiva i poden intentar aturar-la, idealment abans que arribin al seu objectiu.
ISPs (Internet Service Provider)	(ISACA, 2017) Tercer que proporciona a les persones i les empreses accés a internet i una varietat d'altres serveis relacionats amb l'Internet.
KRI (Key Risk Indicator)	(ISACA, 2017) Un subconjunt d'indicadors de risc rellevants que tenen una probabilitat alta de predir o indicar riscos importants.
Log	(ISACA, 2017) Registrar detalls d'informació o esdeveniments en un sistema organitzat de registres, normalment de forma seqüencial en base al moment en què han passat.
Malware	(NIST, 2013) Programa que s'insereix a un sistema, normalment de forma encoberta, amb la voluntat de comprometre la confidencialitat, integritat o disponibilitat de la informació, aplicacions o sistema operatiu de la víctima. També s'utilitza per molestar o interrompre la víctima.
Man-in-the-middle	(NIST, 2013) Atac durant l'execució del protocol d'autenticació en què l'atacant es posiciona entre el sol·licitant i el verificador per a poder interceptar i modificar les dades que s'intercanvien.
Patch	(NIST, 2013) Actualització a un sistema operatiu, aplicació o qualsevol altre software publicat específicament per corregir problemes concrets amb el programari.
Phishing	(NIST, 2013) Enganyar a les persones perquè desvetllin informació sensible de caràcter personal mitjançant medis falsos basats en sistemes informàtics.
Plug-in	(Inc, Accessed 2018) Element del programari s'afegeix a un programa per ajudar amb determinades funcionalitats o característiques.
Port	(NIST, 2013) Entrada física o punt de sortida d'un mòdul criptogràfic que proporciona accés per les senyals físiques al mòdul. Està

	representat per fluxos d'informació lògics (els ports separats físicament no comparteixen el mateix pin o cable físic).
Ransomware	(ISACA, 2017) Malware que restringeix l'accés als sistemes compromesos fins que la demanda de rescat ha estat satisfeta.
RDP	(Inc, Accessed 2018) És un protocol de Microsoft que permet la comunicació en l'execució d'una aplicació entre un terminal i un servidor Windows. Permet l'accés remot a un servidor Windows.
Robatori d'identitat	(ENISA, 2018) Atac que consisteix en què l'atacant obté informació confidencial que s'utilitza per identificar una persona o un sistema informàtic. Subseqüentment aquesta informació és utilitzada per suplantar el propietari de la identitat.
Sandboxing	(NIST, 2013) Entorn restringit, d'execució controlada que evita que codi potencialment maliciós accedeixi a qualsevol sistema excepte a aquells en què el software està autoritzat.
Signatura digital	(ISACA, 2017) Una dada digitalitzada en forma de signatura que proveeix a l'emissor autenticitat, integritat del missatge i no-repudi. Es genera utilitzant la clau privada de l'emissor o aplicant una funció hash d'anada.
SMB Protocol	(Inc, Accessed 2018) És un protocol Windows que permet compartir arxius, impressores i ports en sèrie dins d'una determinada xarxa.
SPAM	(ISACA, 2017) Missatges generats per sistemes informàtics enviats via correu no desitjat.
SQL Injection	(ISACA, 2017) Resultat del fracàs de l'aplicació de validar correctament l'entrada d'informació. Quan l'entrada controlada per l'usuari, especialment dissenyada, consta de sintaxi SQL i s'utilitza sense una validació adequada, és possible obtenir informació de la base de dades de maneres no contemplades durant del disseny de l'aplicació.
SSL (Secure Socket Layer)	(NIST, 2013) Protocol utilitzat per protegir la informació privada durant una transferència via Internet. Nota: SSL funciona utilitzant una clau pública per encriptar les dades que es transfereix sobre la connexió SSL. La majoria dels navegadors web són compatibles amb SSL i moltes pàgines web utilitzen el protocol per obtenir informació confidencial d'usuaris. Per conveni, les URLs que requereixen una connexió SSL comencen amb HTTPS.
TLS (Transport Layer Security)	(NIST, 2013) Un protocol d'autenticació i seguretat implementat de forma general als navegadors i servidors web.
Virus	(NIST, 2013) Programa d'ordinador capaç de replicar-se i d'infectar un ordinador sense permís o coneixement de l'usuari. Un virus pot corrompre o esborrar la informació d'un ordinador, utilitzar serveis

	de correu electrònic per propagar-se cap a altres ordinadors o fins i tot esborrar tot el contingut d'un disc dur.
WAF (Web application Firewall)	(ISACA, 2017) És un plugin de servidor, dispositiu o filtre addicional que pot ser utilitzat per aplicar regles a una aplicació web específica. Supervisa la seguretat web, filtra o bloqueja el tràfic HTTP des de i fins una aplicació web. Opera al nivell 7 de la taula OSI i es pot configurar perquè identifiqui i bloquegi atacs com XSS, SQL injection, etc.
Watering hole attack	(Inc, Accessed 2018) Atac de malware en què l'atacant observa les pàgines web més visitades per la víctima o un grup en concret i infecta aquestes pàgines web. Potencialment, les víctimes s'acabaran infectant.
Web-application atacs	(ENISA, 2018) Atacs dirigits contra les aplicacions web, serveis web i aplicacions mòbils. Se centren en intentar explotar les APIs que estan incorporades a les aplicacions web. Tot i solapar-se amb els atacs basats en la web, en aquest cas el seu abast es limita a l'entorn del temps d'execució i les APIs de les aplicacions web.
Web-based attacks	(ENISA, 2018) Atacs que utilitzen els sistemes habilitats per la web i serveis com ara els navegadors (i les seves extensions), les pàgines web i els components IT dels serveis i aplicacions web.
Whitelist	(NIST, 2013) Llista de diverses entitats, com hosts o aplicacions, que són reconegudes com a benignes i aprovades per ser utilitzades per les organitzacions i/o els sistemes d'informació.
Wi-Fi	(NIST, 2013) Tecnologia que permet la transferència d'informació entre punts separats sense una connexió física.
Worm	(NIST, 2013) Programa auto-contingut capaç d'auto-replicar-se i auto-propagar-se que utilitza mecanismes d'interconnexió de xarxes per propagar-se.

1. Introducció

Fa uns anys que em dedico a la consultoria de riscos en l'àmbit IT (informació i tecnologia). M'he especialitzat en el govern i gestió del risc de ciberseguretat en el sector financer i d'asseguradores. Fonamentalment, el nostre objectiu és protegir la informació crítica del client i els diferents sistemes d'informació que la contenen per tal de garantir la confidencialitat, integritat i disponibilitat.

Durant aquest temps a l'empresa, he vist diferents formes d'atacar els projectes que se'ns proposaven i he utilitzat mètodes diversos per mitigar els riscos existents a les empreses. Com a qualsevol empresa, sempre partia del "know-how" adquirit en projectes anteriors de com s'havia de realitzar la gestió del risc. Però el món de la ciberseguretat està avançant de forma molt ràpida, i amb l'aplicació de la nova llei europea de protecció de dades (GDPR) i la irrupció del cloud computing com a eina per proporcionar serveis informàtics assegurant una reducció de costos per part de les empreses, sembla que el sector està realitzant una revisió de tot el que hi havia desplegat fins ara per assegurar que els clients segueixen estant coberts a nivell de seguretat de la informació amb els controls que tenen aplicats.

D'aquí va sorgir la meva motivació per fer aquest treball. El que em preguntava era: com podem garantir a un client que, amb la migració dels seus sistemes IT al cloud segueix cobert a nivell de seguretat? Apliquen els mateixos controls definits fins al moment o cal incorporar-ne de nous? Realment li suposa una avantatge aquesta migració?

La idea doncs era definir un marc de controls personalitzat que permetés garantir a una empresa del sector financer que volia migrar els seus sistemes al cloud, que estava coberta de les amenaces de ciberseguretat existents actualment no només a nivell legal (pel compliment de la GDPR), sinó també econòmic, de reputació i operacional.

Donat que l'extensió del treball era molt gran, es va decidir abordar-lo conjuntament amb el Miquel Córdoba, company del Màster en Telecomunicacions, per tal de poder extreure'n conclusions més fiables. En aquest sentit, s'ha dividit el projecte en dos grans blocs:

1. El Miquel treballarà la part de la securització d'un entorn on-premise i se centrarà en els fonaments teòrics bàsics pel món de la ciberseguretat, incloent la descripció de les diferents eines disponibles al mercat per la gestió de la ciberseguretat.
2. Jo treballaré la part de la securització d'un entorn cloud i em centraré en conceptes específics de cloud computing, a posar en valor la rellevància d'aquest treball segons l'estat de l'art i a identificar les principals amenaces de ciberseguretat del moment.

D'ara en endavant, es procedirà a explicar el segon bloc. Aquest s'estructurarà de la següent forma:

En primer lloc es definiran els **objectius** del treball. Hi haurà un objectiu principal i quatre objectius secundaris.

En segon lloc es farà un breu resum dels **fonaments teòrics** necessaris per a desenvolupar el treball. Aquests es dividiran bàsicament en dos grans apartats:

- En el primer s'explicarà què s'entén pel govern del risc de ciberseguretat, quins són els principals mètodes existents i els principals conceptes a tenir en compte.
- En el segon s'explicarà què és el cloud computing i quins són els principals models existents i mètodes d'implementació.

En tercer lloc es donarà la instantània de quin és **l'estat de l'art** a dia d'avui. Com en el punt anterior, aquest també tindrà dos grans apartats:

- En el primer s'explicarà què és la ciberseguretat, quina ha estat la seva evolució i quines són les principals amenaces. Després es farà un estudi dels costos derivats dels ciberatacs i la inversió mundial de les empreses per prevenir-los. Per acabar, es mostraran quins són els principals organismes reguladors i no reguladors existents en el mercat i quines són les principals directives, lleis i marcs de control a tenir en compte.
- El segon punt se centrarà en el cloud computing, i es realitzarà el mateix exercici que en el primer punt però específicament per cloud.

Destacar que es considerarà estat de l'art tot allò que porti implícit una temporalitat i fonaments teòrics el que siguin conceptes a priori definitius.

En quart lloc s'explicarà la **metodologia** proposada per tal de realitzar el cas pràctic: l'anàlisi de riscos de seguretat. Primer es justificarà l'ús d'aquesta metodologia i després es farà una descripció detallada de tots els passos a seguir per la realització d'un anàlisi de riscos que ens permeti avaluar el risc residual que haurà d'acceptar l'empresa després de l'aplicació del marc de controls definits.

En cinquè lloc es realitzarà el **cas pràctic** on es procedirà a securitzar la migració al cloud de l'Office365 mitjançant la implementació de les mesures de seguretat corresponents. L'objectiu és proposar una solució que compleixi amb els requeriments de seguretat demanats per l'entitat. Per fer-ho, es realitzarà un anàlisi de riscos pels tres escenaris possibles identificats:

1. Accés directe a Office 365 tenint en compte només els propis controls de Microsoft.
2. Accés directe a Office365 amb controls addicionals per donar compliment als requeriments de seguretat.
3. Accés a Office365 mitjançant la xarxa corporativa de l'entitat.

En base als resultats obtinguts es farà una proposta de les mesures de seguretat a afegir per mitigar els riscos fins a un nivell acceptable i així donar compliment als requeriments demanats per l'entitat.

En sisè lloc s'extrauran les **conclusions** del treball, que tindran en compte:

- Els resultats obtinguts al cas pràctic.
- La comparativa amb la solució on-premise dissenyada pel Miquel Córdoba, company del Màster en Telecomunicacions.
- La valoració del compliment dels objectius.

En setè lloc es comentaran les **línies de futur** del treball.

En vuitè lloc s'inclourà la **bibliografia** amb totes les fonts citades durant el projecte.

Per últim s'afegirà un apartat de **recursos** on es pot trobar el full de càlcul utilitzar per la realització de l'anàlisi de riscos del cas pràctic i la memòria realitzada pel Miquel Córdoba, company del màster en Telecomunicacions.

2. Objectius

L'objectiu principal del projecte és analitzar la diferència de nivell de risc de seguretat al què està exposat una empresa del sector financer segons si utilitza una solució cloud o una solució on-premise per desplegar els diferents sistemes IT.

Recordar que, com s'ha comentat en la Introducció, aquest projecte està dividit en dos treballs: en un es realitza l'anàlisi del nivell de risc de seguretat utilitzant una solució cloud i en l'altre es realitza el mateix exercici però utilitzant una solució on-premise.

En aquest projecte, es realitzarà l'anàlisi del nivell de risc de seguretat utilitzant una solució cloud per l'Office365. Per tal d'assolir l'objectiu, es defineixen els següents **objectius secundaris**:

1. La identificació dels principals riscos y amenaces de seguretat actuals que puguin comprometre la confidencialitat, integritat o disponibilitat dels diferents sistemes IT: infraestructura, aplicacions, arquitectura, comunicacions, gestió d'identitats i processos definits.
2. La definició d'un marc de controls que permeti garantir la integritat, confidencialitat i disponibilitat de la informació en un entorn cloud.
3. L'avaluació de la capacitat de resposta i resiliència dels sistemes anteriors enfront a incidents de seguretat un cop aplicats els controls proposats.
4. L'avaluació de la continuïtat del negoci dels sistemes anteriors enfront a incidents de seguretat un cop aplicats els controls proposats.

3. Fonaments teòrics

3.1. Govern del risc de ciberseguretat

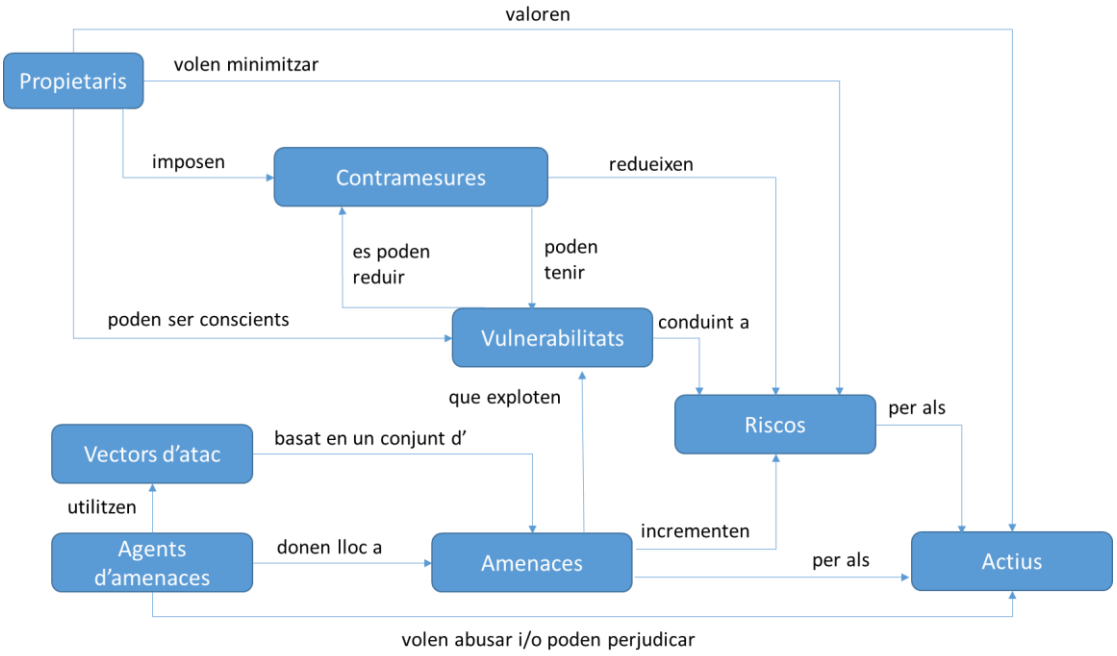
(ISACA, 2017) S'entén per govern de la ciberseguretat, la responsabilitat que té el comitè de direcció d'una organització d'assegurar que, mitjançant un marc de controls d'estàndards i processos definit, es garanteix la securització de l'organització enfront al ciberrisc.

3.1.1. Conceptes clau per la gestió del risc

(ISACA, 2017) La funció clau de la ciberseguretat és identificar, mitigar i gestionar el ciberrisc dels actius digitals d'una organització. A mode glossari, a sota, s'identifiquen uns quants termes que ens serviran a posteriori per realitzar aquesta gestió del risc:

- **Impacte**: (ISACA, CRISC Review Manual, 2015) mesura la magnitud del dany resultat de l'explotació d'una vulnerabilitat. Pot ser financer, de reputació o legal.
- **Probabilitat**: (ISACA, CRISC Review Manual, 2015) mesura la freqüència en què un esdeveniment pot succeir. Dependrà de si hi ha una font potencial per a que passi (amenaça) i en quina mesura podrà afectar un determinat tipus d'esdeveniment al seu objectiu (vulnerabilitat). A més també caldrà tenir en compte els controls implementats per l'organització per tal de reduir aquesta vulnerabilitat.
- **Amenaça**: (ISACA, 2017) qualsevol cosa (objecte, substància, persona,...) que sigui capaç d'actuar en contra d'un actiu ocasionant un dany.
- **Actiu**: (ISACA, 2017) cosa tangible o intangible que té un valor que es considera significatius i cal protegir. Inclou persones, informació, infraestructura, finances i reputació.
- **Vulnerabilitat**: (ISACA, 2017) debilitat en el disseny, implementació, operació o control intern d'un procés que podria exposar un sistema a les amenaces externes.
- **Risc**: (ISO, 2005) combinació de la probabilitat que passi un esdeveniment i l'impacte que se'n deriva. El risc és mitigat mitjançant l'ús de controls o salvaguardes.
  (ENISA, 2018) Per aquest treball, considerarem que el risc està format per:
  Actiu (Vulnerabilitats, Controls), **Amenaça** (Perfil de l'agent d'amenaça, probabilitat) i **Impacte**.
- **Risc inherent**: (ISACA, 2017) nivell de risc existent sense tenir en compte les accions que el negoci prendrà o pren per tal de mitigar-lo.
- **Risc residual**: (ISACA, 2017) nivell de risc restant després d'aplicar les mesures de seguretat acordades amb la direcció.

A continuació es mostra de forma gràfica la relació entre els diferents elements del risc.

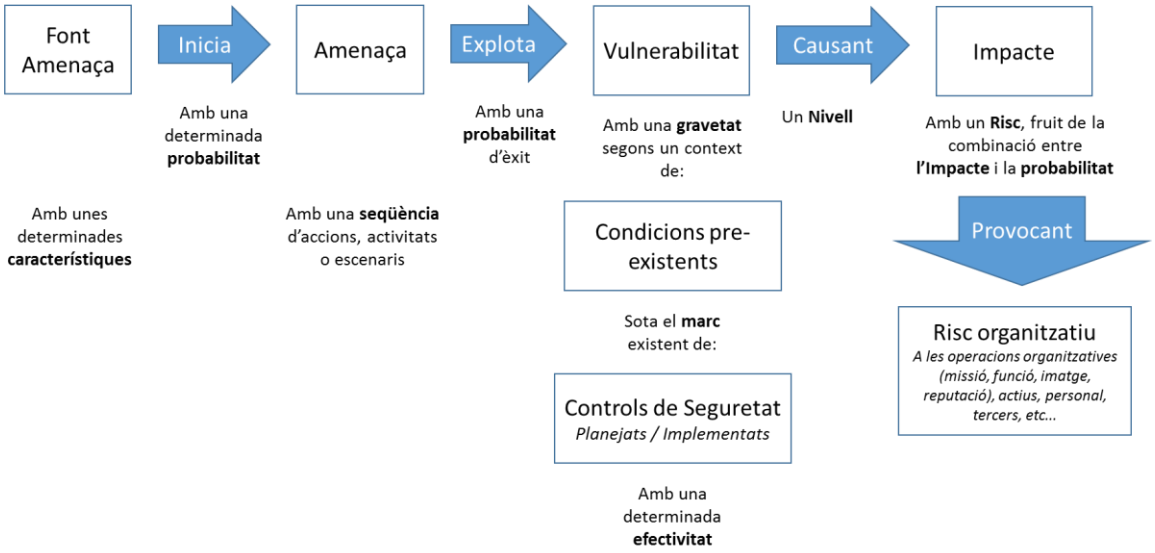


Il·lustració 1. Relació entre els diferents elements del risc. (ENISA, 2018).

3.1.2. Formes d'enfocar la gestió del risc

(ISACA, 2017) Un escenari de risc és la descripció d'un possible esdeveniment que tindrà un impacte incert sobre els objectius que vol assolir una empresa (pot ser negatiu o positiu). El desenvolupament d'escenaris de risc es basa en la descripció del risc potencial i la documentació dels factors / àrees que es poden veure afectats pel mateix. Cada escenari estarà relacionat amb un objectiu de negoci o un impacte (p.e. robatoris, pèrdua de les credencials personals, fallada del sistema, etc.).

A sota s'explica de forma gràfica en què consisteix la gestió del risc:



Il·lustració 2. Gestió del risc. (National Institute of Standards and Technology, 2012)

Hi ha dues maneres d'arribar a definir aquests escenaris de risc:

- **Mètode descendent** (*top-down)*:
  Es basa en el coneixement dels objectius de negoci i com un esdeveniment pot afectar la consecució d'aquests objectius. Sota aquest model, es mira quin seria el resultat si succeïssin aquests esdeveniments que posarien en perill els objectius definits per la direcció de negoci. Destacar que és un mètode que s'utilitza per la gestió general del risc, tant IT com no IT.

- **Mètode ascendent** (*bottom-up):*
  Es basa en la descripció d'esdeveniments de risc específics de ciberseguretat. És una bona manera d'identificar escenaris on hi ha una dependència molt alta en el funcionament tècnic d'un sistema o d'un procés.
  A vegades, seguint aquest mètode és més complicat mantenir l'interès de la capa més alta de negoci.

Cal destacar que és molt important tenir en compte el nivell de tolerància al risc que té una organització abans de realitzar l'anàlisi. Així doncs, no serà el mateix resultat l'anàlisi per una institució acadèmica o un petit negoci que per un banc.

De cara a la realització d'aquest treball, s'utilitzarà el mètode ascendent per tal de centrar-nos en els riscos específics de ciberseguretat.

3.1.3. Formes de respondre al risc

(ISACA, 2017) Existeixen 4 formes de respondre a tots aquells riscos que no disposen de controls o que aquests són inadequats:

- **Reduir el risc** mitjançant la implementació de controls mitigants que redueixin la probabilitat o l'impacte del risc dins del nivell de tolerància de l'empresa.
- **Evitar el risc,** per exemple, no participant en una activitat o negoci concret.
- **Transferir o compartir el risc**. El risc es pot transferir a un tercer, com podria ser una asseguradora o es pot compartir amb un tercer via un acord contractual.
- **Acceptar el risc**. Sempre i quan el risc estigui dins dels nivells de tolerància de l'empresa o que el cost d'implementació dels controls mitigants sigui més alt que les pèrdues potencials que es derivarien del risc.

3.1.4. Formes d'enfocar un anàlisi de riscos de ciberseguretat

(ISACA, 2017) Es considera que hi ha tres formes diferents de realitzar un anàlisi de riscos a nivell de ciberseguretat:

- **Ad-hoc**
  Implementar mesures de seguretat sense un criteri particular. Aquest mètode reflecteix un insuficient coneixement de la matèria i falta d'entrenament en el disseny i la implementació de controls mitigatoris.
- **Basat en el compliment de certs estàndards**
  Es basa en normatives o estàndards existents per determinar la implementació de les mesures de seguretat. Els controls s'implementen sense tenir en compte la seva aplicabilitat o necessitat.

- **Basat en el risc**
  Es basa en la identificació dels riscos particulars que té una organització a l'hora de dissenyar i implementar els controls de seguretat que mitigaran el risc. També té en compte el nivell de tolerància al risc que té cada organització i les necessitats reals de negoci.

Normalment s'utilitza una combinació dels dos últims mètodes: basat en el compliment de certs estàndards i basat en el risc. I aquesta és la proposta que s'utilitzarà en aquest treball a l'hora de realitzar l'anàlisi de riscos.

Destacar que molts estàndards com ara la ISO27001, el PCI DSS (Payment Card Industry Data Security Standard), SOX (Sarbanes-Oxley Act) ja requereixen de la realització d'un anàlisi de riscos per la implementació dels controls requerits.

3.1.5. Principals agents d'amenaça actuals a nivell de ciberseguretat

(ENISA, 2018) Les amenaces són creades per uns agents d'amenaça que actuen de forma organitzada i voluntària per atacar actius considerats importants / sensibles i exploten vulnerabilitats a través de certs vectors d'atac. Els principals agents d'amenaça descrits per ENISA a tenir en compte, per ordre d'importància en relació al panorama anterior d'amenaces, són:

3.1.5.1. Cibercriminals

(ISACA, 2017) Els motiva l'afany de lucre, aquests individus estan involucrats en transaccions financeres fraudulentes. (ENISA, 2018) Durant l'any 2017 han estat el grup més actiu, sent els responsables d'almenys dues terceres parts dels incidents registrats a Europa. Els atacs perpetrats són sobre actius amb un alt valor i estan altament personalitzats, demanant sempre una compensació econòmica.

3.1.5.2. Empleats

(ISACA, 2017) Encara que típicament disposen d'eines i mètodes de baixa tecnologia, empleats actuals o passats insatisfets presenten un risc alt de ciberseguretat. (ENISA, 2018) Tot i encara ser el segon grup principal, el 2017 ha estat el primer any on s'ha observat una baixada en l'activitat. Dins dels empleats hi ha dos grups, els que ho fan de forma intencionada i els no-intencionats. Els primers busquen, fonamentalment, una compensació econòmica, sent el sector de la salut el més perjudicat. Els segons, acostumen a ser víctimes d'atacs com ara phishing, fet que fa augmentar molt el percentatge d'empleats que causen incidents de seguretat.

3.1.5.3. Estats

(ISACA, 2017) Els estats acostumen a tenir com a objectiu entitats governamentals o polítiques amb un gran nivell de sofisticació per obtenir intel·ligència o dur a terme altres activitats destructives. (ENISA, 2018) Segons l'informe de l'any 2017, han esdevingut el tercer agent d'amenaça amb més del 20% dels incidents. Donada la gran capacitat d'aquest grup, els atacs normalment són complicats d'identificar i defensar.

3.1.5.4. Hacktivists

(ISACA, 2017) Tot i que normalment actuen de forma independent, els hackers motivats per raons polítiques poden atacar persones o organitzacions específiques per aconseguir fins ideològics. (ENISA, 2018) És un grup on hi ha un nivell tant d'eines com de capacitats i coneixements molt diferent entre els individus.

3.1.5.5. Ciberguerrers

(ISACA, 2017) Es tracta de ciutadans motivats que actuen en nom d'un partit polític o una religió en contra un altre partit polític que els està amenaçant.

3.1.5.6. Ciberterroristes

(ISACA, 2017) Es caracteritzen per la seva predisposició d'utilitzar violència per aconseguir els seus objectius. Normalment ataquen infraestructures crítiques i grups governamentals.

3.1.5.7. Script Kiddies

(ISACA, 2017) Individus que estan aprenent a hackejar. Poden treballar sols o amb altres i normalment es caracteritzen per realitzar injeccions de codi o atacs DDoS.

3.1.5.8. Empreses

(ISACA, 2017) Algunes empreses traspassen els límits de la seguretat i realitzen actes maliciosos per aconseguir un avantatge competitiu.

A continuació es mostra una taula que permet veure gràficament la implicació dels diferents agents de seguretat envers les principals amenaces (el detall de les principals amenaces existents es pot trobar al punt 4.4).

🔴 Grup primari per l'amenaça
🟢 Grup secundari per l'amenaça

Taula 1. Implicació dels agents de seguretat en les principals amenaces. (ENISA, 2018).

AMENACES	AGENTS D'AMENAÇA							
	Cibercriminals	Empleats	Estats	Empreses	Hacktivists	Ciberguerrers	Ciberterroristes	Script Kiddies
Malware	🔴	🟢	🔴	🔴	🟢	🟢	🟢	🟢
Web-based atacs	🔴		🔴	🔴	🔴	🔴	🔴	🟢
Web-application atacs	🔴		🔴	🔴	🔴	🔴	🟢	🟢
Phishing	🔴	🔴	🔴	🔴	🔴	🔴		
Spam	🟢	🔴	🟢	🟢				
Denegació de servei (DoS)	🔴		🟢	🟢	🔴	🔴	🟢	🔴
Ransomware	🔴	🟢	🔴	🔴		🟢		🟢
Botnets	🔴		🔴	🔴	🟢	🔴		🟢
Amenaça interna	🔴		🟢	🔴		🟢	🟢	
Manipulació física, danys, pèrdues, robatoris	🔴	🔴	🔴	🔴	🟢		🟢	🟢
Filtració de dades	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢
Robatori d'identitat	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢
Fuga d'informació	🔴		🔴	🔴	🟢	🟢	🟢	🟢
Exploit kits	🔴		🔴	🔴		🟢		
Ciber-espionatge		🟢	🔴	🔴		🟢		

3.1.6. Principals vectors d'atac

Un cop descrites les principals amenaces i agents d'amenaça, ens faltaria per veure quins són els vectors d'atac que utilitzen per poder explotar les vulnerabilitats i atacar els seus objectius.

(ENISA, 2018) Començarem per definir un vector d'atac com el mitjà utilitzat per l'agent d'amenaça per explotar les vulnerabilitats existents sobre els actius (inclosos els humans) per assolir un resultat específic.

Mètodes d'atac

Les principals tècniques utilitzades com a vectors d'atac serien:

- Malware
  - Virus
  - Network worm
  - Trojan Horses
  - Botnets
  - Spyware
  - Adware
  - Ransomware
  - KeyLogger
  - Rootkit
- APT
- Backdoor
- Atacs de força bruta
- Buffer overflow
- Cross-Site Scripting (XSS)
- Atacs DoS
- Atacs man-in-the-middle
- Enginyeria Social
- Phishing
- Spear phishing
- Spoofing
- SQL Injection
- Zero-day exploit
- Watering hole
- Exploit kits
- Eines d'accés remot (RAT)

Nota: La descripció de cada un d'ells es pot trobar al glossari.

Canals d'atac

Alguns exemples de possibles canals d'atac són (ENISA, 2018):

- Atacant l'element humà
- Atacs a través de la web, aplicacions web i navegadors
- Atacs a través dels actius exposats a Internet
- Explotació de vulnerabilitats o configuracions errònies i defectes dels protocols de seguretat a nivell de criptografia i xarxa
- Atacs a través de la cadena de subministrament
- Propagació per la xarxa/moviments laterals
- Atacs a la xarxa activa
- Atacs a la xarxa passiva
- Fuga d'informació
- Atacs smokescreen
- Botigues d'aplicacions mòbils
- USB maliciosos
- Card skimming

3.2. Cloud Computing

3.2.1. Definició

(Badger, Grance, Patt-Corner, & Voas, 2012) Segons el NIST SP 800-145, el cloud computing és un model que permet accés via la xarxa de forma convenient i sota petició a un grup compartit de recursos informàtics configurables (p.e. xarxes, servidors, sistemes d'emmagatzematge, aplicacions i serveis) que es poden aprovisionar i alliberar ràpidament amb un mínim esforç de

gestió o d'interacció amb el proveïdor. Aquest model al núvol està format per 5 característiques essencials, tres models de servei i quatre models d'implementació.

3.2.2. Característiques essencials

(Badger, Grance, Patt-Corner, & Voas, 2012) Les principals característiques són:

- **Self-service sota petició**
  Un usuari pot aprovisionar unilateralment les capacitats informàtiques que necessiti de forma automàtica sense requerir interacció humana amb cada proveïdor de servei.
- **Ampli accés a la xarxa**
  Les capacitats estan disponibles a la xarxa i són accessibles mitjançant mecanismes estàndards que promouen l'ús de plataformes thin o thick client (p.e. telèfons mòbils, tauletes, ordinadors portàtils, ordinadors fixes).
- **Agrupació de recursos**
  Els recursos informàtics del proveïdor estan agrupats per poder ser utilitzats per múltiples clients, utilitzant un model de multi-tenant, amb recursos físics i virtuals diferents, assignats i re-assignats de forma dinàmica sota demanda de l'usuari. L'usuari generalment no té control o coneixement sobre la localització exacte dels serveis proveïts. Exemples de recursos podrien ser sistemes d'emmagatzematge, processament, memòria i ample de banda de la xarxa.
- **Flexibilitat**
  Les capacitats poden ser aprovisionades de forma ràpida i flexible, en alguns casos de forma automàtica, per poder escalar cap amunt o cap avall ràpidament de manera proporcional a la demanda. Per a l'usuari, les capacitats disponibles per a l'aprovisionament sovint semblen ser il·limitades i es poden adquirir en qualsevol quantitat i en qualsevol moment.
- **Escalabilitat**
  Els serveis cloud controlen i optimitzen automàticament l'ús de recursos aprofitant una capacitat d'escalabilitat adequada al tipus de servei (p.e. emmagatzematge, processament, ample de banda i comptes d'usuari actives). L'ús de recursos es pot monitoritzar, controlar i informar proporcionant transparència tant al proveïdor com a l'usuari del servei utilitzat.

3.2.3. Models de servei

Existeixen tres models de servei cloud: SaaS, PaaS i IaaS. A continuació es procedirà a donar més detall de cada un d'ells.

3.2.3.1. Cloud Software as a Service (SaaS)

(Badger, Grance, Patt-Corner, & Voas, 2012) La capacitat proporcionada a l'usuari és utilitzar les aplicacions del proveïdor que s'executen sobre una infraestructura cloud. En aquest sentit:

- Les aplicacions són accessibles des de diversos dispositius de client mitjançant una interfície de thin client com ara un navegador web (p.e. correu electrònic basat en la web), o una interfície de programa.
- L'usuari no gestiona o controla la infraestructura cloud subjacent, incloent la xarxa, els servidors, el sistema operatiu, l'emmagatzematge o fins i tot les capacitats individuals de l'aplicació (amb l'excepció de configuracions específiques de l'usuari).

(ISACA & CSA, Cloud Computing Market Maturity, 2015) El prefereixen la petita i mitjana empresa, que valoren el model de "paga pel que utilitzes" pel desplegament de les aplicacions que sinó haurien de desplegar, testejar i mantenir ells amb recursos a les seves pròpies

instal·lacions. Utilitzant aplicacions basades en cloud (p.e. serveis de correu electrònic, impressores, ...) poden invertir el seu capital en el desenvolupament de les seves competències base.

És el model més adoptat, sobretot a nivell del mercat de cloud públic, sent les aplicacions de Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), recursos humans, sistemes d'inventari i sistemes de gestió de nòmines, les més utilitzades.

3.2.3.2. Cloud Platform as a Service (PaaS)

(Badger, Grance, Patt-Corner, & Voas, 2012) La capacitat proporcionada a l'usuari és desplegar a la infraestructura del núvol les aplicacions creades o adquirides pels consumidors que han estat desenvolupades utilitzant llenguatges de programació i eines compatibles amb el proveïdor cloud. En aquest sentit:

- L'usuari no administra ni controla la infraestructura del núvol subjacent, incloent la xarxa, els servidors, el sistema operatiu, l'emmagatzematge.
- Però té control sobre les aplicacions implementades i possiblement les configuracions d'entorn host d'aplicacions.

(ISACA & CSA, Cloud Computing Market Maturity, 2015) El prefereixen les grans empreses que necessiten recursos per desenvolupar i testejar noves aplicacions. Adoptant un model PaaS, poden experimentar amb noves tecnologies i nous serveis que si s'haguessin d'implementar a la infraestructura de l'empresa i no al cloud, requeririen d'una inversió a la que no podrien fer front. Amb l'ús del cloud, les empreses es poden adaptar ràpidament als canvis del mercat i complir amb l'expectativa de la demanda.

És el model que més està creixent. Permet a les empreses reduir el temps de desplegament d'aplicacions pròpies ja que els projectes es poden llençar sense necessitat d'esperar el desenvolupament i testeig de recursos interns com ara servidors, xarxes, dispositius de back-up, infraestructura de seguretat, etc.

3.2.3.3. Cloud Infrastructure as a Service (IaaS)

(Badger, Grance, Patt-Corner, & Voas, 2012) La capacitat proporcionada a l'usuari és processament, emmagatzematge, xarxes i altres recursos informàtics fonamentals on l'usuari pugui implementar i executar software arbitrari, que pot incloure sistemes operatius i aplicacions. En aquest sentit:

- L'usuari no gestiona ni controla la infraestructura subjacent del núvol.
- Però té control sobre els sistemes operatius, l'emmagatzematge i les aplicacions desplegades i possiblement un control limitat dels components de xarxa seleccionats (p.e. firewalls host).

(ISACA & CSA, Cloud Computing Market Maturity, 2015) Permet a les empreses, com en el cas anterior, experimentar amb noves tecnologies i nous serveis. Segons sembla, a futur, s'acabarà ajuntant amb el model PaaS per oferir un model més robust i complet.

3.2.4. Models d'implementació

(Badger, Grance, Patt-Corner, & Voas, 2012) Els diferents models d'implementació són:

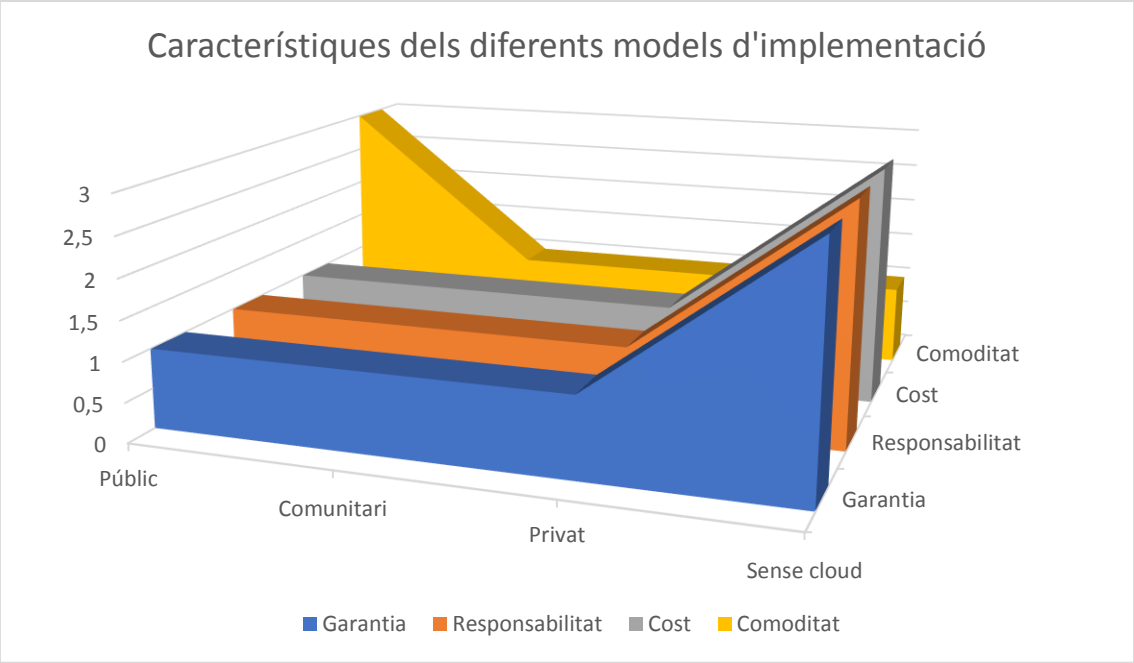
Taula 2. Models d'implementació del cloud computing. (Badger, Grance, Patt-Corner, & Voas, 2012)

Model	Descripció
Cloud privat	- La infraestructura cloud s'aprovisiona per ús exclusiu d'una organització formada per múltiples consumidors (p.e. diferents unitats de negoci). - Pot ser que sigui propietat, ser administrada i operada per l'organització, un tercer o alguna combinació. - Pot existir dins o fora de les instal·lacions.
Cloud comunitari	- La infraestructura cloud s'aprovisiona per l'ús exclusiu d'una comunitat d'usuaris específica d'organitzacions que tenen preocupacions compartides (p.e. una missió, requeriments de seguretat, polítiques i marc normatiu, etc...). - Pot ser que sigui propietat, ser administrada i operada per una o varies de les organitzacions dins la comunitat, un tercer o una combinació. - Pot existir dins o fora de les instal·lacions.
Cloud públic	- La infraestructura cloud s'aprovisiona per l'ús obert del públic general. - Pot ser que sigui propietat, ser administrada i operada per una organització acadèmica, governamental o privada, o una combinació. - Existeix a les instal·lacions del proveïdor de serveis cloud.
Cloud híbrid	- La infraestructura cloud és una combinació de dos o més infraestructures cloud diferents (privada, comunitària o pública) que segueixen sent entitats úniques però estan unides per una tecnologia estandarditzada o patentada que permet la transferència de dades i aplicacions.

(ISACA & CSA, Cloud Computing Market Maturity, 2015) El cloud privat i el cloud híbrid l'utilitzen fonamentalment les grans empreses que han d'integrar tecnologia ja existent amb productes cloud o fins i tot que tenen requeriments legals i de compliment que limiten l'adopció dels clouds públics.

El model de cloud comunitari està desapareixent i s'està treballant amb un model que permeti a les empreses col·laborar però sense necessitat de formar part del mateix cloud comunitari.

La relació entre comoditat, cost, responsabilitat i garantia dels diferents clouds varia segons la gràfica següent:



Il·lustració 3. Característiques dels diferents models d'implementació de serveis cloud. (ENISA, 2009)

3.2.5. Seguretat al cloud

(ISACA & CSA, Cloud Computing Market Maturity, 2015) Les empreses adopten serveis cloud perquè esperen reduir els costos i tenir un entorn IT més escalable i flexible que els permeti mantenir el creixement del seu negoci.

(Right Scale, 2018) Segons l'enquesta més recent realitzada per Right Scale, la primera preocupació dels usuaris de serveis cloud és com es garanteix la seguretat. A continuació, els preocupa: la gestió de la despesa, la manca de recursos / coneixement, el govern i control del cloud, el compliment normatiu, la gestió de múltiples clouds, el rendiment i com construir un cloud privat.

A continuació, doncs, es farà un petit estudi de quins són els beneficis que aporta un servei cloud a nivell de seguretat i, per contra, quins són els riscos que es generen.

3.2.5.1. Beneficis dels serveis cloud a nivell de seguretat

(ENISA, 2009) Els principals beneficis del cloud a nivell de seguretat són:

- **Escalabilitat:** qualsevol mesura de seguretat serà més barata implementada a gran escala. Per això, per la mateixa inversió en seguretat es pot garantir una millor protecció (filtratge, gestió de patches, hardening de màquines virtuals i hypervisors, etc..). Addicionalment, el fet de tenir xarxes edge permet proporcionar el contingut més a prop de la seva ubicació, que provoca un temps de resposta més ràpid i una millor gestió d'amenaces i incidents.
- **La seguretat per diferenciar-se en el mercat:** com s'ha comprovat en el punts anteriors, la seguretat és la primera preocupació dels usuaris de serveis cloud a l'hora d'adquirir-los. Per tant, els usuaris es basaran en la reputació a nivell de confidencialitat, integritat i disponibilitat oferta pel proveïdor. Això obliga als proveïdors de cloud a millorar els controls de seguretat que ofereixen per mantenir-se competitius.

- **L'estandardització** dels serveis de seguretat crea un mercat de serveis de seguretat més ampli i a punt per ser utilitzat.
- **Disponibilitat:** l'habilitat que té el proveïdor de cloud de redistribuir dinàmicament els recursos permet garantir una disponibilitat molt més elevada.
- **Auditoria:** es poden emmagatzemar logs de forma més eficient i es poden consultar imatges forenses de les màquines virtuals sense fer caure els sistemes.
- **Actualitzacions:** es poden instal·lar de forma més ràpida, efectiva i eficient les actualitzacions a nivell de seguretat i evitar les configuracions que venen per defecte.
- **Concentració de recursos:** tot i suposar un risc a nivell de seguretat, també permet reduir els costos a nivell de controls d'accés físic i reduir el cost dels processos de seguretat.

3.2.5.2. Principals riscos de seguretat dels serveis cloud

(INCIBE, 2016) Dins dels serveis emergents, el cloud computing es considera el principal objectiu de les ciberamenaces. Això és degut principalment a les següents característiques:

- La utilització de recursos compartits.
- El personal del proveïdor de cloud i els seus dispositius que també tenen accés potencial a les dades.
- Els tercers contractats pel proveïdor de cloud.
- L'accessibilitat als proveïdors de cloud i la seva exposició.
- L'alta quantitat de dades que emmagatzemen els proveïdors cloud.

(ENISA, 2009) A conseqüència d'aquestes característiques, es deriven els següents riscos de seguretat dels serveis cloud:

- **Pèrdua del govern:** a l'utilitzar infraestructures del cloud, l'usuari cedeix el control al proveïdor de cloud en certes qüestions que afecten la seguretat. A més, si aquestes qüestions no estan incloses en el Service Level Agreement (SLA) es pot produir un GAP important de seguretat.
- **Lock-In:** actualment existeix poca oferta a nivell d'eines, procediments, formats de dades estàndard o interfícies de servei que puguin garantir la portabilitat de les dades, aplicacions i serveis entre proveïdors cloud. Això pot dificultar al client migrar d'un proveïdor a un altre o migrar dades i serveis a un entorn informàtic intern. Això introdueix una dependència envers al proveïdor de cloud, especialment si la portabilitat de dades no està habilitada.
- **Errors d'aïllament:** multi-tenancy i recursos compartits són característiques essencials d'un entorn cloud. El risc es produeix, doncs, si fallen els mecanismes que permeten la separació d'emmagatzematge, memòria, enrutament o reputació entre diferents tenants *(guest-hoping-attacks)*. No obstant això, cal tenir en compte que els atacs als mecanismes d'aïllament de recursos (p.e. hipervisors) són poc nombrosos i molt més difícils que els atacs als sistemes operatius tradicionals.
- **Compliment normatiu:** hi pot haver el risc de no complir amb els estàndards de seguretat quan es migra a un entorn cloud ja sigui perquè el proveïdor no pot donar l'evidència del compliment amb els requeriments rellevants, o bé perquè el proveïdor no permet rebre auditories per part de l'usuari. En certs casos, fins i tot l'ús d'un cloud públic farà que no es compleixi amb l'actual marc normatiu, com seria el cas de PCI DSS.
- **Compromís de la gestió de l'interfície:** la gestió de les interfícies de l'usuari d'un proveïdor de cloud públic són accessibles via Internet i donen accés a conjunts de

recursos més grans que els proveïdors d'allotjament tradicionals). Per tant, suposen un augment del risc, especialment quan es combinen amb l'accés remot i les vulnerabilitats del navegador web.

- **Protecció de dades:** en alguns casos és complicat que l'usuari del servei cloud, com a figura de controlador de les dades, pugui comprovar de forma efectiva les pràctiques de tractament de dades del proveïdor del núvol i, per tant, assegurar-se que les dades es tractin de manera lícita. Aquest problema s'agreuja en els casos de transferències múltiples de dades, per exemple, entre núvols federats. D'altra banda, alguns proveïdors proporcionen informació sobre les pràctiques de manipulació de dades o resums de certificació en les seves activitats de processament de dades i seguretat de dades i els controls que tenen en marxa.
- **Esborrat de dades no segur o incomplet:** quan es fa una petició d'esborrat d'un recurs del cloud, pot resultar en un esborrat no segur de les dades. L'eliminació de dades de forma adequada o a temps pot no ser possible degut a, per exemple, que les còpies addicionals de les dades no estan disponibles o perquè el disc a destruir conté dades d'altres clients. Pels casos de multi-tenancy i de reutilització de recursos hardware, aquest punt representa un risc més alt que per clients amb infraestructura dedicada.
- **Atacant intern:** el mal que poden causar els atacants interns d'un proveïdor cloud és molt superior. Les arquitectures cloud necessiten certs rols que presenten un risc molt alt. Per exemple, els administradors de sistemes i els proveïdors que gestionen els serveis de seguretat.

Remarcar que aquests riscos surten de comparar-ho amb una solució "on-premise" i que no estan ordenats per importància.

3.2.5.3. Capacitats de Seguretat Cloud

A continuació, es detallen un seguit de capacitats de seguretat que permeten la securització dels entorns cloud.

3.2.5.3.1. Mobile Device Management (MDM)

(Sherweb, 2018) Actualment, les empreses proporcionen als seus treballadors una gran varietat de dispositius mòbils, d'entre els que trobem telèfons, tablets i ordinadors portàtils. Una necessitat bàsica pels administradors de seguretat és poder controlar aquests dispositius en remot d'una forma unificada. Aquest procés s'executa a través del que s'anomena Mobile Device Management o MDM, un procés en el que els administradors IT configuren polítiques per tal d'optimitzar la seguretat i la funcionalitat d'aquests dispositius dins de la organització.

(Microsoft, 2018) Les polítiques establertes per l'MDM s'envien a través del núvol cap als agents que tenen instal·lats els dispositius i permeten tenir un gran control sobre el seu ús, permetent principalment les següents funcionalitats:

- Bloqueig remot del dispositiu.
- Sol·licitud de contrasenya i doble factor d'autenticació.
- Bloqueig del dispositiu per inactivitat.
- Rastreig del dispositiu.
- Xifrat de la informació del dispositiu.
- Detecció i prevenció de la modificació del dispositiu (jailbreak o root).
- Creació de còpies de seguretat.
- Esborrat remot de dades.

- Limitació de funcionalitats pròpies del dispositiu.

Utilitzant aquest tipus de solucions, les organitzacions poden tenir sempre informació actualitzada sobre tots els seus dispositius, sigui quina sigui la seva ubicació. També permet prevenir els riscos derivats de la mobilitat, que són les connexions a xarxes no segures o les pèrdues o robatoris de dispositius.

(Sherweb, 2018) Totes aquestes funcionalitats fan de les solucions MDM una eina molt efectiva per mitigar un gran nombre de riscos derivats de la utilització de dispositius mòbils, cosa que, segons Gartner, ha portat a dos terços de les empreses a nivell mundial a utilitzar aquest tipus de solucions.

3.2.5.3.2. Bring Your Own Key (BYOK)

(Thales, 2018) Una de les desavantatges del cloud a nivell de seguretat és el fet de que les dades s'emmagatzemin dins de les instal·lacions del proveïdor de serveis cloud i fora del control del propietari d'aquestes. Moltes organitzacions opten per xifrar les seves dades per tal d'evitar-ho, però aquesta solució comporta securitzar correctament la clau de xifrat utilitzada. La funcionalitat Bring Your Own Key (BYOK) permet a les organitzacions xifrar les seves dades i mantenir el control de la gestió de les seves claus de xifrat.

(Rouse, 2018) Utilitzant BYOK, els clients de serveis cloud poden utilitzar una versió virtualitzada del seu software de xifrat juntament amb les aplicacions de negoci que utilitzen en aquest entorn per tal de xifrar les dades. D'aquesta manera, l'entorn es configura per tal de que totes les dades siguin processades pel software de xifrat i aquest les pugi al cloud ja xifrades. Si l'usuari necessita accés a aquestes dades, es realitza el procés invers per desxifrar-les. Aquesta manera de treballar proporciona a les organitzacions el control sobre les seves pròpies claus, la possibilitat de generar-les mitjançant els mètodes que considerin més segurs i aporta un grau aparent de seguretat de cara als propietaris de les dades ja que les claus de xifrat s'emmagatzemen als seus propis sistemes.

Així doncs, la funcionalitat principal de BYOK és reduir el risc de fuga d'informació en entorns cloud, però més enllà d'això el que també busca és aportar aquesta sensació o percepció de seguretat als propietaris de les dades emmagatzemades al saber que el proveïdor de cloud no té accés directe a les seves dades. Aquesta manera de treballar facilita també la securització d'una migració des d'un proveïdor cloud cap a un altre, al aportar un major grau de confidencialitat de la informació migrada, tot i que no té cap impacte en la integritat, ja que no podrà evitar que, per exemple, es perdi una unitat d'informació durant la migració.

3.2.5.3.3. Rights Management Service (RMS)

(Microsoft, 2018) Azure Rights Management Service (sovint abreviat com Azure RMS) és la tecnologia de Microsoft utilitzada dins del conjunt de capacitats d'Azure Information Protection per oferir solucions de protecció de documents. Aquest servei de protecció basat en el cloud utilitza directives de xifrat, identitat i autorització per protegir documents ja sigui a dins de l'organització o a fora, ja que la protecció sempre es manté juntament amb les dades, tot i que aquestes es trobin fora dels límits de la organització.

Azure RMS funciona xifrant els documents, etiquetant-los i incloent-hi una política que defineix quins usuaris poden utilitzar-los i quin ús en poden fer. Aquesta funcionalitat permet utilitzar diferents tipus de xifrat pels documents en funció de les necessitats i de la robustesa requerida i aporta un alt grau de control a l'organització sobre els documents que comparteix ja que en qualsevol moment pot gestionar qui hi accedeix, assignar una caducitat als documents o fins i

tot "eliminar" el document (realment el document no s'elimina, el que s'elimina es la clau per desxifrar-lo, cosa que el fa totalment inservible).

(Encamina, 2018) A nivell general, RMS presenta les següents avantatges:

- Permet l'accés de treballadors, proveïdors i clients als documents de l'organització i el revoca si deixen la empresa.
- Enviament de documents amb la garantia de que únicament el destinatari els podrà obrir.
- Control d'accés granular per grups, usuaris i dominis.
- Seguiment en temps real de l'activitat dels documents protegits (quan, com i qui els obre, des de quina localització...).
- Aplicació de regles de seguretat pels documents protegits.

3.2.5.3.4. Active Directory Federation Services (ADFS)

(Microsoft, 2018) Actualment els usuaris d'una organització accedeixen a multitud de recursos, aplicacions i serveis ubicats tant a dins com a fora dels límits de la seva pròpia empresa. Aplicacions gestionades per proveïdors o per clients, recursos externs i serveis al cloud, tots ells requereixen una autenticació per part d'aquests usuaris, que pot arribar a ser poc àgil si aquests han d'utilitzar credencials i identitats diferents per a cadascun d'aquests serveis i si cada cop que entren han de perdre temps en identificar-se.

ADFS és un component software desenvolupat per Microsoft que permet proporcionar accés als usuaris a diversos sistemes dins o fora dels límits de la organització utilitzant una única instància d'autenticació (el que s'anomena single sign-on). Aquest objectiu s'assoleix compartint les dades d'identitat d'un usuari entre un grup de diverses entitats confiables (conegut com "federació"). Quan un usuari requereix accés a una aplicació propietat d'una entitat part de la federació, la pròpia organització de l'usuari és responsable d'autenticar a l'usuari i de proporcionar la informació necessària que determini la seva identitat enviant sol·licituds cap a la organització responsable de l'aplicació. Aquesta organització utilitza llavors una política de confiança per concedir l'autorització a l'aplicació en qüestió.

Aquesta funcionalitat permet als usuaris no haver-se d'identificar i iniciar sessió cada cop que accedeixen a diferents aplicacions, recursos i serveis, facilitant les seves tasques, agilitzant l'autenticació i estalviant temps alhora que es garanteix la correcta gestió de les identitats i el control d'accessos.

3.2.5.3.5. Cloud Access Security Broker (CASB)

Els serveis al núvol continuen experimentant un gran creixement i la migració cap al cloud és una tendència a la majoria d'organitzacions, principalment, per les avantatges que ofereix en quant a l'accés a la informació o a les aplicacions des de qualsevol dispositiu amb accés a Internet. Aquesta flexibilitat però, comporta també riscos de seguretat importants si no es controlen aquests entorns i s'implementen capacitats de seguretat adaptades a les particularitats dels serveis cloud.

(Mendoza, Miguel Ángel, 2018) Els CASB (o Cloud Access Security Brokers) sorgeixen com una necessitat per atendre els riscos de seguretat derivats de proveïdors cloud, especialment en el model SaaS (o Software com a servei) que implica la utilització de software emmagatzemat i gestionat dins dels servidors del propi proveïdor. Són eines de seguretat orientades a protegir d'atacs contra les dades i contra els usuaris d'aquest tipus de serveis, però amb l'avantatge de que són gestionats per la pròpia organització. La ubicació dels CASB doncs, és entre els usuaris i

els proveïdors de serveis cloud, amb l'objectiu de combinar i intercalar les polítiques de seguretat pròpies de la empresa amb els mètodes d'accés als recursos del cloud.

Així doncs, la principal característica d'aquests sistemes és que operen al punt mig entre les aplicacions al núvol i els usuaris, amb l'objectiu de proporcionar visibilitat (registres d'auditoria, alertes de seguretat, informes) i seguretat a les dades (a través de controls d'accés, prevenció de la fuga d'informació i xifrat, entre d'altres).

L'arquitectura i els components d'un CASB varien molt d'un proveïdor a un altre, però generalment es basen en un mecanisme Proxy sobre el que es construeix la solució. D'aquesta manera, es disposa de la capacitat d'inspeccionar tot el tràfic que passa pel dispositiu i permet conèixer les activitats que realitzen els usuaris que utilitzen el servei. Cal destacar que no només es busca protegir l'accés al núvol i la informació que s'emmagatzema, la protecció d'aquestes eines es considera des del moment en el que es genera la informació, per tant els CASB incorporen mètodes de classificació d'informació, xifrat de dades sensibles o accessibilitat a la informació restringida a determinats usuaris.

Finalment, és important tenir en compte com en la resta de solucions de seguretat, que el desplegament d'una infraestructura d'aquest tipus suposa un impacte directe sobre les aplicacions i dispositius afectats i per tant haurà d'estar dimensionada i adaptada als requeriments de l'organització i dels usuaris, buscant l'equilibri entre operació i protecció.

3.2.5.3.6. CISCO Email Security (CISCO-CES)

(CISCO, 2018) Dins de les eines específiques per protegir el servei de correu corporatiu, trobem l'eina CES (CISCO Email Security) del fabricant CISCO. Aquesta solució proporciona funcionalitats de seguretat per prevenir els principals riscos que afecten al correu, entre les que podem destacar les següents:

- **Protecció i detecció de Phishing**, per identificar recipients maliciosos per tal de bloquejar-los.
- **Protecció de dominis,** per prevenir que els atacants puguin utilitzar el domini d'una organització per realitzar atacs de phishing.
- **Protecció específica per Office 365,** proporcionant un sistema de defensa robust contra el ransomware, la fuga d'informació, els atacs de phishing i d'altres.
- **Escaneig d'arxius,** per tal d'identificar documents potencialment perillosos i la presencia de programari maliciós.

(Fernandez, 2018) Donada la naturalesa oberta i descentralitzada del SMTP, la suplantació (*spoofing*) de correus electrònics és un problema comú. En aquest sentit, CISCO CES té la capacitat d'implementar les següents mesures de defensa per evitar la suplantació d'identitat:

- **SPF** (Sender Policy Framework): els registres del conveni de remitents indiquen al destinatari quins són els serveis d'allotjament o direccions IP que poden enviar e-mails al seu domini.
- **DKIM** (Domain Keys Identified Mail): és un mètode d'autenticació de correu que verifica criptogràficament si un correu electrònic ha estat enviat per servidors autoritzat i no ha estat modificat en trànsit.
- **DMARC** (Domain-based Message Authentication, Reporting and Conformance): és una capa addicional a la configuració del SPF i al DKIM que permet al propietari del domini especificar què ha de passar amb tots aquells correus electrònics que no són verificats.

4. Estat de l'art

4.1. La ciberseguretat

La ciberseguretat forma part de la seguretat de la informació, però es centra específicament en la protecció de tots els actius digitals (maquinari de xarxa, programari i tot els sistemes d'informació interconnectats per xarxes). No inclou, doncs, les catàstrofes naturals o la seguretat física que sí que formarien part del terme general de seguretat de la informació.

Hi ha moltes possibles definicions per la paraula **ciberseguretat**, al ésser un terme relativament nou i encara en constant evolució. Per exemple:

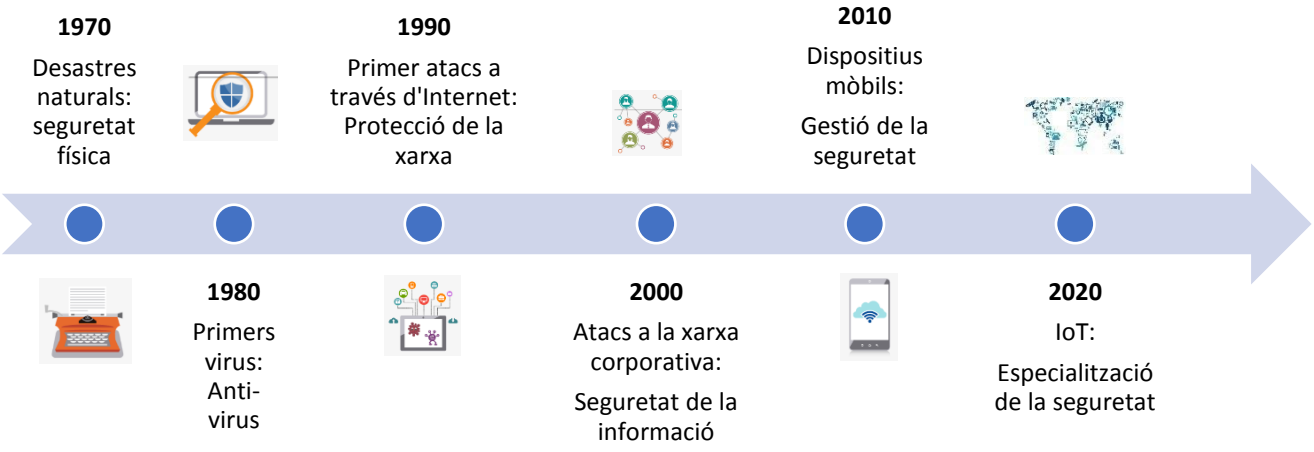
- (Cybersecurity, 2017) El fet d'estar protegit de l'ús criminal o no autoritzat de dades electròniques o les mesures adoptades per aconseguir-ho.
- (ISACA, 2017) La protecció dels actius que contenen informació mitjançant la gestió de les amenaces existents per tota aquella informació processada, guardada o transportada mitjançant sistemes d'informació interconnectats per xarxes.

4.2. Evolució de la ciberseguretat

La preservació de la informació ha estat una prioritat des que les persones han necessitat guardar la seva informació de forma segura i privada.

(INCIBE, 2015) Fins la dècada dels 70, la seguretat de les empreses estava centrada en garantir el bon ús de la informació per part dels empleats. Amb la introducció de la tecnologia a les empreses, però, la seguretat va evolucionar cap a nous objectius.

Fent un repàs històric dels punts claus que representen avenços o canvis significants en les tendències tecnològiques, ens apareixen les següents etapes:

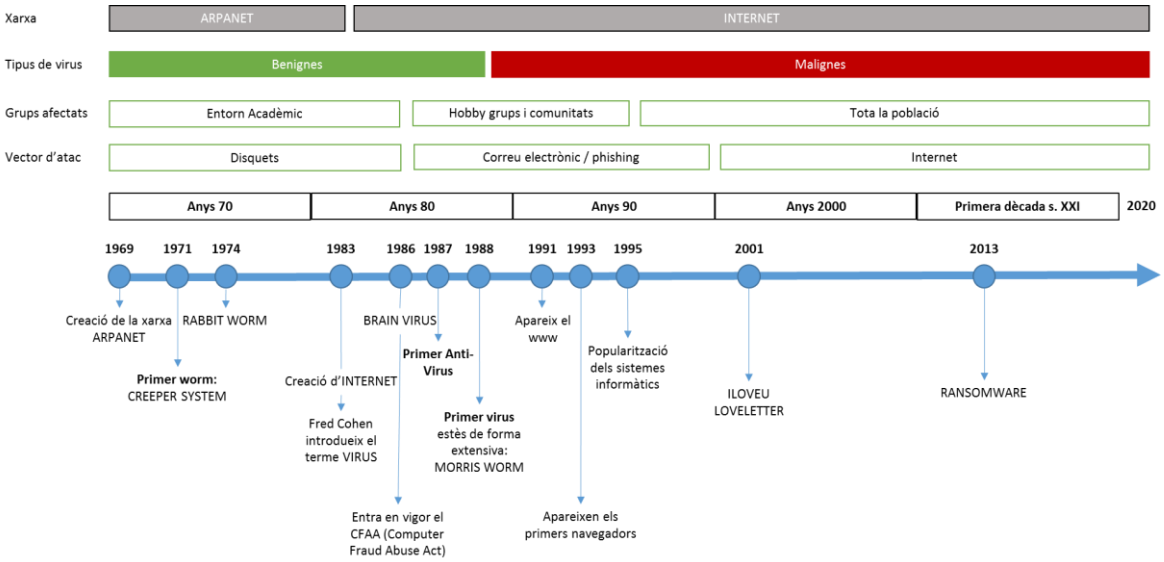


Il·lustració 4. Evolució de la seguretat. (INCIBE, 2015)

Podríem afirmar que la necessitat de la ciberseguretat apareix amb la popularització de l'Internet. De fet, fou amb l'aparició de les xarxes que interconnectaven dispositius (primer l'ARPANET i posteriorment Internet), que van començar a aparèixer els primers virus i *worms*. (Chen, 2004) que es caracteritzen fonamentalment per la seva capacitat d'auto-replicar-se. (Khanse, 2014) Els primers virus i worms eren innocus tant pels usuaris com pels sistemes informàtics. Estaven dissenyats com a bromes pesades o per donar a conèixer els seus creadors. Amb el pas del temps, però, els creadors de malware han començat a utilitzar les seves creacions

per fins maliciosos, com ara el robatori de credencials bancàries, enviament de missatges spam, suborns, etc.

Podríem dir que les principals fites relacionades amb la ciberseguretat es descriuen en el següent gràfic:



Il·lustració 5. Evolució de la ciberseguretat.

(Julian, 2014) (INCIBE, 2015) (Khanse, 2014)

Durant els **anys 70**, hi havia poques mesures de seguretat desplegades i totes elles eren físiques. L'any 1971 va aparèixer el primer worm informàtic a la xarxa ARPANET, el creeper. No es tractava d'un malware com a tal ja que només mostrava un missatge a l'usuari i no era capaç d'auto-replicar-se. En aquella època, els empleats eren poc coneixedors dels riscos associats a la informació que manipulaven.

Durant els **anys 80**, la majoria dels virus informàtics es trobaven a la universitat i la propagació es feia majoritàriament via disquets. L'any 1983 podríem dir que va néixer Internet com a tal i Fred Cohen va introduir per primera vegada el terme virus. El primer virus fou el Brain, que tenia com a objectiu arribar a les comunitats i grups que tenien com a hobby la informàtica. Es propagava mitjançant disquets i també només mostrava un missatge a l'usuari.

L'any 1986 entra en vigor el Computer Fraud Abuse Act, que prohibeix legalment accedir a un ordinador sense autorització. Robert Morris fou el primer en ser acusat per crear l'any 1988, el Morris worm, que va ocasionar danys en infectar més de 5000 ordinadors als EEUU.

A partir d'aquest moment, els sistemes informàtics van començar a disposar d'algunes mesures de seguretat i es comencen a comercialitzar els anti-virus.

Durant els **anys 90**, els virus es comencen a fer virals (valgui la redundància) i virus com el Melissa o ILOVEYOU van ser capaços d'infectar desenes de milions de PCs, provocant la fallada dels sistemes de correu electrònic d'arreu. A més, es comença a invertir molt en la tecnologia *anti-malware* i es comença a treballar en la conscienciació social, especialment en temes de prevenció de *phishing*.

Durant els **anys 2000**, els atacs es comencen a dirigir a les eines encarregades de protegir la informació i la xarxa corporativa. Es produeix la primera gran filtració de dades (45,7 milions de números de targetes de crèdit), que li provocà unes pèrdues d'uns 256 milions a la companyia americana TJX. Arrel d'això, es comença a regular la seguretat de la informació per part de les empreses i aquestes es comencen a dotar de sistemes de seguretat més sofisticats d'acord amb les amenaces existents (p.e. comencen a dotar cada un dels seus sistemes d'anti-virus).

A més també es comença a popularitzar l'ús de les xarxes socials, apareixen riscos de seguretat derivats d'empleats insatisfets i es comencen a produir fraus online.

A partir d'aquest moment i fins **l'actualitat**, es produeix un boom i comencen a aparèixer tot tipus de malware (Spyware, adware, trojans, rootkits, ransomware, etc...). És a partir d'aleshores que les empreses comencen a posar el focus en la ciberseguretat en resposta a tots els ciberatacs rebuts. En aquest sentit, apareixen plans sòlids de conscienciació dels empleats sobre la seguretat de la informació i lleis de protecció d'infraestructures crítiques; es realitza un major control sobre la privacitat de la informació per evitar-ne les fugues i es fa ús d'eines d'encriptació d'informació a nivell corporatiu i personal.

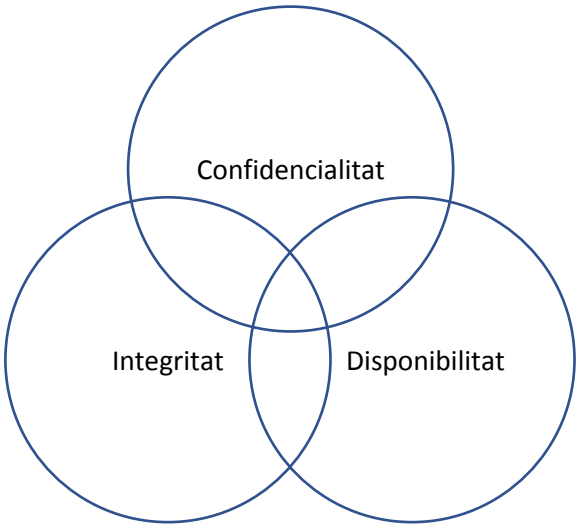
Addicionalment, es treballa en la securització dels dispositius mòbils, que disposen de poques mesures de seguretat que impedeixin la fuga de la informació corporativa.

(World Economic Forum, 2018) Actualment, segons un estudi del World Economic Forum, a nivell mundial el risc de ciberatacs es troba en tercera posició a nivell de probabilitat i en sisena posició a nivell d'impacte, per darrera, fonamentalment, dels riscos mediambientals com ara els desastres naturals.

4.3. Objectius de la ciberseguretat

(ISACA, 2017) Actualment, l'objectiu de la ciberseguretat és triple i pretén mantenir la confidencialitat, integritat i disponibilitat de les dades. Aquests termes es poden definir com:

- **Confidencialitat**: protecció dels accessos no autoritzats o divulgació de la informació. Destacar que la informació ha de ser protegida segons la seva sensibilitat i en base als requeriments legals que l'apliquin. Fonamentalment es garanteix mitjançant controls d'accés robustos, encriptació i permisos sobre els arxius.
- **Integritat**: protecció de la modificació no autoritzada de les dades. Bàsicament es garanteix mitjançant logs, signatures digitals, hashes, encriptació i controls d'accés.
- **Disponibilitat:** assegura la no interrupció en l'accés a les dades. La fiabilitat de l'accés en tot moment a les dades es pot garantir mitjançant redundància, back-ups i la implementació de plans de continuïtat del negoci.



Il·lustració 6. Tripleta de la Ciberseguretat. (ISACA, 2017).

També és important destacar el **no-repudi**, que fa referència al concepte d'assegurar que un missatge o una dada és genuïna. És a dir, quan s'envia la informació és important verificar que prové de la font que apareix. El no-repudi permet a la persona que rep/emet un missatge confirmar que efectivament és aquella persona. S'implementa mitjançant la signatura digital i el *log* transaccional.

4.4. Principals amenaces actuals a nivell de ciberseguretat

(ENISA, 2018) L'estratègia a nivell de ciberseguretat proposada per la unió europea, destaca la importància d'analitzar les amenaces i les tendències emergents en el món de la ciberseguretat. En aquest sentit, i segons l'informe anual del 2017 de l'ENISA, actualment les 15 principals amenaces a nivell de ciberseguretat a tenir en compte són:

Nota: en cas de necessitar-ho, la definició de cada terme es troba al Glossari.

.

Taula 3. Principals amenaces de ciberseguretat. (ENISA, 2018)

Núm.	Amenaces	Possibles controls mitigants	Estadístiques	Tendència
1	**Malware** (p.e. WannaCry, NotPetya, atacs RDP, CrySIS, vulnerabilitat EternalBlue, etc..)	- Sistemes de detecció de malware actualitzats, tant als dispositius finals com a tots els canals de comunicació, tant d'entrada com de sortida (sistemes de xarxa, web i d'aplicació) incloent totes les plataformes (PC, dispositius mòbils, infraestructura de xarxa). - Establir interfícies de detecció de malware amb funcions de gestió d'incidents de seguretat per establir un temps eficient de resposta. - Desenvolupar polítiques de seguretat que especifiquin el procés a seguir en cas d'infecció. - Revisió d'antivirus i d'actualitzacions de forma periòdica.	- Aproximadament 22 milions de noves mostres de malware s'han detectat al primer trimestre del 2017. - És l'amenaça que més incidents genera a l'any.	
2	**Web-based atacs** (p.e. Explotació del navegador web o una de les seves extensions, explotació dels serveis o servidors web, water-holing, redireccionaments)	- Ús de mecanismes de protecció dels navegadors (sandboxing, extensió anti-malware) i canviar la configuració per defecte. - Evitar els plugins / extensions de fonts no confiables. - Filtrat del tràfic web (blacklisting) i ús de tecnologies d'encriptació de tràfic (SSL/TLS). - Actualització i patching de forma periòdica dels navegadors web. - Protecció dels dispositius finals de programari no actualitzat que conté vulnerabilitats. - Monitorització del comportament del software per detectar comportament maliciosos (plugins).	- >50% de tots els ciberatacs tenen com a objectiu o utilitzen tecnologies basades en la web. - 58% de la distribució del malware es fa via descàrregues web.	

Núm.	Amenaces	Possibles controls mitigants	Estadístiques	Tendència
3	**Web-application atacs** (p.e. SQL Injection, Cross-site Scripting (XSS), ...)	- Ús de mecanismes d'autenticació i autorització adequats. - Instal·lació de WAF (Web application Firewalling). - Filtratge del tràfic de tots els canals rellevants (web, xarxa, correu). - Creació de polítiques de seguretat pel desenvolupament i la operativa de les aplicacions. - Verificació de la font de la informació i gestió de l'ample de banda disponible. - Realització d'escanejos de vulnerabilitats i de detecció d'intrusions de forma periòdica. - Corregir vulnerabilitats del codi durant el desenvolupament i no a producció.	- Hi ha aproximadament 1.8 bilions de mitjana d'atacs diaris, dels quals hi ha 6298 deteccions d'explotació de vulnerabilitats.	
4	**Phishing**	- Conscienciació i educació del personal de l'empresa perquè identifiquin els correus maliciosos o falsos i no cliquin sobre enllaços no segurs. - Utilització de gateways de correu específics per filtrar spam. - Utilitzar el doble factor d'autentificació sempre que sigui possible. - Utilitzar una política de contrasenyes segura.	- És el responsable d'entre el 90 i el 95% d'atacs duts a terme de forma satisfactòria a nivell mundial. - Es creen aproximadament un milió de pàgines web de phishing al mes.	

Núm.	Amenaces	Possibles controls mitigants	Estadístiques	Tendència
5	**Spam**	- Conscienciació i educació del personal de l'empresa perquè identifiquin els correus maliciosos o falsos i no cliquin sobre enllaços no segurs. - Ús de DKIM (Domain keys Identified Mail, filtres de reputació, filtres de contingut. - Ús de la intel·ligència artificial per detectar anomalies. - Bloqueig dels executables (i macros) que es troben en els adjunts dels correus. - Deshabilitar l'execució automàtica de codi, macros, rendering dels gràfics i pre-càrrega de links en els correus.	- A l'últim trimestre del 2017, un 85% del total de correu diari era spam. - El 88% de l'spam és enviat per botnets.	
6	**Denegació de servei** (DoS) p.e. APDoS, DNS water torture, SSL atacs, PdoS, IoT Botnets	- Creació d'una política de seguretat respecte DoS i DdoS i també d'un pla de detecció i gestió d'incidents. - Ús d'ISPs. - Triar de mesures de protecció tècniques anti-DdoS (a nivell de firewall, ACLs, balancejadors de càrrega, IPS/WAF, IDMS, ...). - Anàlisi i documentació dels proveïdors utilitzats. - Implementació d'un sistema IPS per la correcta identificació d'atacs d'intrusió.	- >33% de les empreses han patit un atac DDoS aquest 2017 (20% petites empreses, 33% pimes i un 41% grans empreses). - La indústria més atacada és la del joc, amb un 80% del tràfic.	

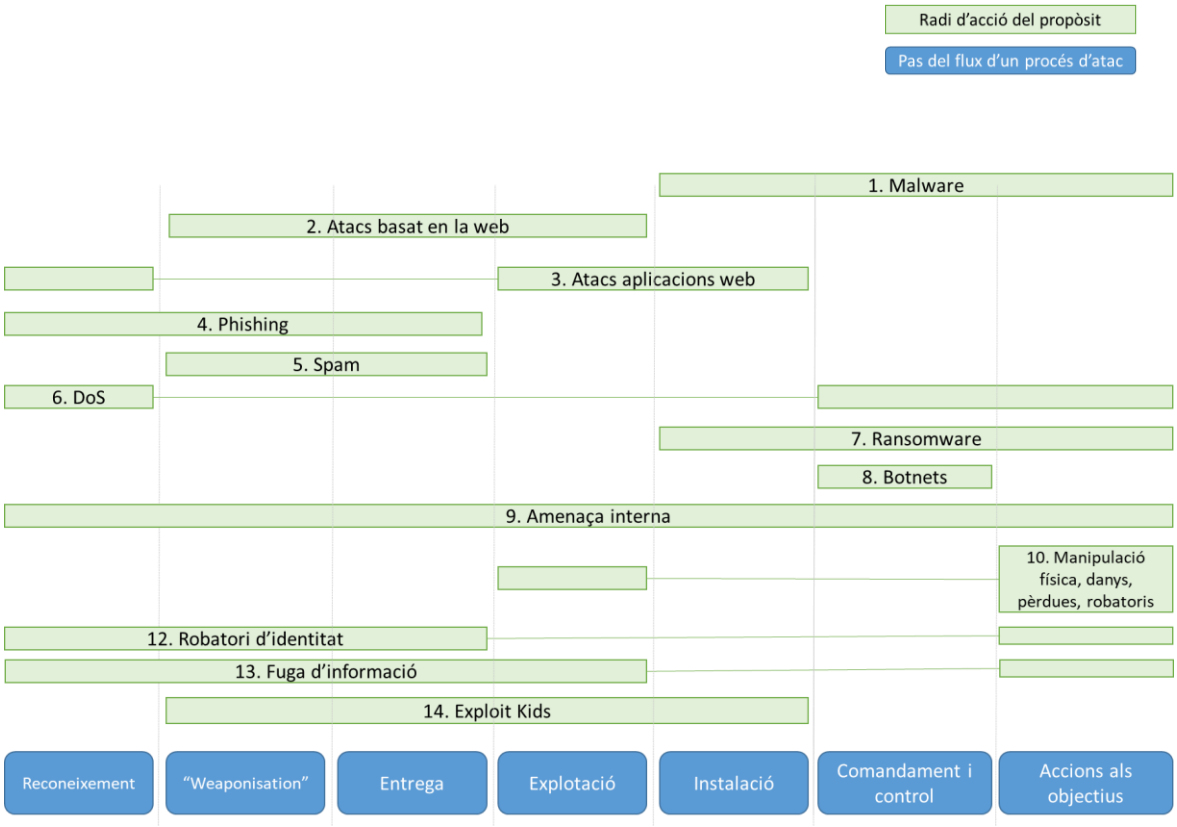
Núm.	Amenaces	Possibles controls mitigants	Estadístiques	Tendència
7	**Ransomware** p.e. cerber, jaff, sage, globelmposter, locky	- Control d'accés limitat als usuaris mínims i autoritzats. - Gestió de vulnerabilitats i actualitzacions de "patches" periòdiques. - Ús d'anti-virus actualitzats. - Ús de back-ups amb la capacitat de recuperació de les dades en el temps establert. - Implementació del filtrat de continguts en correu electrònic i tràfic de xarxa. - Control l'accessibilitat a nivell de ports dels dispositius externs. - Utilitzar llistes blanques per permetre els arxius executables. - Conscienciació del personal de l'empresa.	- El 60% de les infeccions de malware són ransomeware. - El 71% de les companyies objectiu de ransomware són infectades. - 2/3 parts de les infeccions de ransomware al primer trimestre de 2017 es van introduir via RDP.	
8	**Botnets** P.e. Necurs, the Reaper,	- La majoria de botnets s'utilitzen per realitzar atacs de DdoS, per tant, cal tenir en compte sobretot els controls mitigants del punt 6 d'aquesta mateixa taula. - Instal·lació i configuració de sistemes de firewall d'aplicació i de xarxa. - Filtratge del tràfic de tots els canals rellevants (xarxa, web i correu electrònic). - Manteniment d'una llista negra d'Ips. - Realització d'escanejos de vulnerabilitats.	- Hi ha hagut un increment d'un 69,2% de l'ús del malware respecte l'últim trimestre de 2016. - >2 milions de dispositius són vulnerables i podrien ser infectats.	
9	**Amenaça interna** p.e. Bases de dades, sistemes d'arxius, dispositius mòbils	- Conscienciació del personal de l'empresa. - Definició de polítiques internes a nivell de seguretat de la informació. - Ús de solucions d'IAM per la implementació de la segregació de funcions segons els rols. - Control d'accés només pel personal autoritzat i basat en rols.	- El principal problema el presenten els usuaris administradors. - Un 74% de les empreses se senten vulnerables als atacs interns. - Un 88% de les empreses ha posat en marxa sistemes de detecció.	

Núm.	Amenaces	Possibles controls mitigants	Estadístiques	Tendència
10	**Manipulació física, danys, pèrdues, robatoris**	- Ús de l'encriptació de tota la informació emmagatzemada i aquella que està fora del perímetre de seguretat (dispositius, xarxes, serveis cloud, etc.). - Utilitzar inventaris per fer un seguiments dels dispositius existents. - Seguretat física per l'accés a zones on hi ha informació sensible. - Implementació de polítiques de seguretat física.	- Les accions físiques estan presents en un 8% de les violacions de les dades. - Un 18% de les violacions de dades són causades per pèrdues accidentals. - De mitjana les persones perden 1,24 objectes a l'any amb informació sensible.	
11	**Filtració de dades** P.e. DU Group, NetEase, River City Media, LLC; Deep Root Analytics, Edmodo, EmailCar, etc...	- Classificació de les dades en funció de la sensibilitat per poder aplicar les mesures de seguretat adequades. - Implementació de solucions DLP per protegir les dades tant en trànsit com en repòs. - Encriptació de les dades sensibles en trànsit i en repòs. - Control d'accés reduït al principi de menors privilegis necessaris per realitzar les funcions del lloc de treball corresponent. - Gestió de vulnerabilitats adequada i instal·lació i actualització de les mesures d'anti-malware. - Creació de polítiques de seguretat, especialment a nivell de contrasenyes. - Ús del doble factor d'autenticació. - Limitar la informació sensible emmagatzemada en aplicacions accessibles des d'Internet. - Conscienciació del personal de l'empresa amb les polítiques de seguretat establertes.	- El nombre elevat de filtracions de dades a causa de contrasenyes forçades o robades han reduït a molt baixa la capacitat de protecció d'aquests. - Després de l'aplicació de la llei GDPR els danys causats per la pèrdua de dades tindran greus repercussions. - Un 35,4% dels atacs tenien com a objectiu empreses del sector mèdic.	

Núm.	Amenaces	Possibles controls mitigants	Estadístiques	Tendència
12	**Robatori d'identitat** p.e. dumpster divers, phishers, hackers, ...	- Protegir amb un bon control d'accés tots els documents d'identitat (físics i digitals). - Configurar polítiques de privacitat adequades. - Creació de polítiques de seguretat, especialment a nivell de contrasenyes. - Parar atenció a les xarxes públiques de Wi-Fi. - Instal·lació d'anti-malware als dispositius finals i correcta actualització. - Utilitzar eines de prevenció de fuga d'informació (DLP).	- Al regne unit, es roben unes 500 identitats per dia. - La informació de targetes de crèdit està disponible online a partir de 10-20$ i representa un 33% dels robatoris. - Casi un 80% de la població no ho considera un risc / preocupació.	
13	**Fuga d'informació** p.e. cloudbleed, voter records, Macron campaign, etc...	- Realització de revisió del codi de forma periòdica i solució de vulnerabilitats descobertes. - Classificació de les dades en funció de la sensibilitat per poder aplicar les mesures de seguretat adequades. - Implementació de solucions DLP per protegir les dades tant en trànsit com en repòs. - Encriptació de les dades sensibles en trànsit i en repòs - Control d'accés reduït al principi de menors privilegis necessaris per realitzar les funcions del lloc de treball corresponent. - Gestió de vulnerabilitats adequada i instal·lació i actualització de les mesures d'anti-malware. - Creació de polítiques de seguretat, especialment a nivell de contrasenyes. - Ús del doble factor d'autenticació. - Conscienciació del personal de l'empresa.	- El factor humà (error) és el principal motiu de fuga d'informació. - La fuga d'informació s'ha vist incrementada per l'aparició d'aplicacions mòbils. - La principal preocupació relacionada amb BYOD era la fuga d'informació (69%).	

Núm.	Amenaces	Possibles controls mitigants	Estadístiques	Tendència
14	**Exploit kits** p.e. angler, Magnitude, Nuclear	Aplicarien els mateixos controls que pel cas 1 (malware), tot i que en destaquen els següents: - Gestió de vulnerabilitats adequada i instal·lació i actualització de les mesures d'anti-malware. - Sistemes de detecció de malware actualitzats tant als dispositius finals com a tots els canals de comunicació, tant d'entrada com de sortida (sistemes de xarxa, web i d'aplicació) incloent totes les plataformes (PC, dispositius mòbils, infraestructura de xarxa). - Ús d'un gateway segur a nivell de correu electrònic amb filtres de contingut (anti-spam, anti-malware, etc...).	- No hi ha hagut canvis destacats en les infeccions per exploit kits. - S'espera que el seu ús es redueixi considerablement en un futur pròxim.	
15	**Ciber-espionatge** p.e. CopyKittens, APT33, APT32, etc..	- Identificació dels rols crítics d'una organització i anàlisi de riscos a nivell de negoci. - Creació de polítiques de seguretat que incloguin pràctiques de conscienciació del personal, govern corporatiu i seguretat operacional. - Desenvolupament de KPIs per fer un seguiment del compliment de les polítiques i adaptar-se als possibles canvis. - Gestió de vulnerabilitats adequada i instal·lació i actualització de les mesures d'anti-malware. - Sistemes de detecció de malware actualitzats tant als dispositius finals com a tots els canals de comunicació, tant d'entrada com de sortida (sistemes de xarxa, web i d'aplicació) incloent totes les plataformes (PC, dispositius mòbils, infraestructura de xarxa). - Control d'accés reduït al principi de menors privilegis necessaris per realitzar les funcions del lloc de treball corresponent (basat amb el concepte "need-to-know").	- Un 20% de les organitzacions a nivell mundial el consideren el risc principal al seu negoci. - Als estats units, un 20% de les empreses han patit atacs de ciber espionatge.	

Dins de l'estructura d'un atac, les diferents amenaces es trobarien en el següent lloc:



Il·lustració 7. Abast de les amenaces dins d'un atac. (ENISA, 2018).

(ISACA, 2017) Tot i que les principals amenaces són intencionades, també hi ha altres tipus d'amenaces que poden ajudar a que es produeixi un ciberatac com ara:

- Mala gestió de la informació crítica o sensible per part dels usuaris autoritzats.
- Configuració errònia dels privilegis.
- Vulnerabilitats pre-existents al programari instal·lat.
- Errors de disc o altres problemes causats per l'envelliment dels equips.
- Desastres naturals com ara foc, inundacions, huracans, terratrèmols a les ubicacions primàries o de back-up.

Per tal de protegir els sistemes enfront a aquestes amenaces, existeixen diversos marcs de control i normatives que ajuden a les empreses a mantenir un nivell de seguretat adequat en funció de la informació i els sistemes existents.

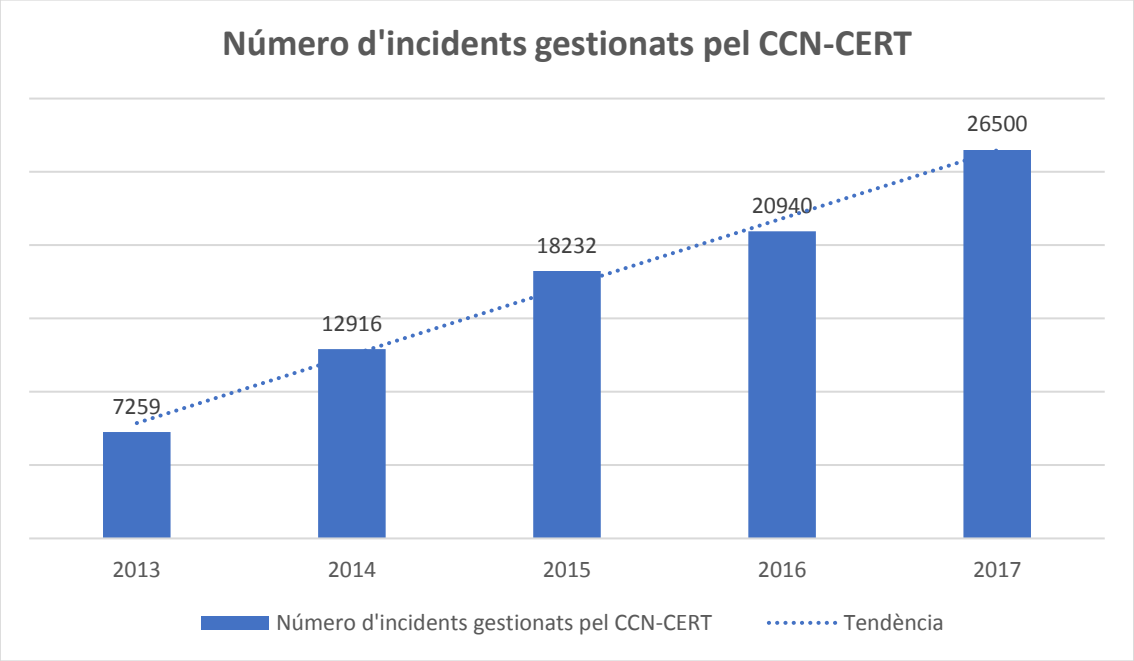
En el nostre cas, ens centrarem en el marc de controls definit pel NIST per tal d'assegurar que s'avaluen correctament totes les amenaces i que s'apliquen els controls mitigants adequats per tal de reduir el risc a un nivell acceptable.

4.5. Incidents de ciberseguretat

(UE, 2018) Segons un estudi realitzat per la unió europea, el 80% de les empreses han patit com a mínim un ciberatac durant aquest any passat. Més de 150 països i 230000 sistemes de tots els sectors s'han vist afectats amb un impacte alt en els serveis essencials com ara hospitals i ambulàncies.

De fet, l'any 2016 es van registrar més de 4.000 atacs de ransomware per dia, amb un increment d'un 38% respecte l'any anterior. En alguns països membres de la UE, el 50% de tots els crims comesos són cibercrims.

(CCN-CERT, 2017) A nivell espanyol, el creixement de ciberatacs gestionats pel CCN-CERT s'ha incrementat un 26,55% aquest darrer any. A sota es mostra una gràfica amb l'evolució dels diferents incidents de ciberseguretat gestionats pel CCN-CERT.

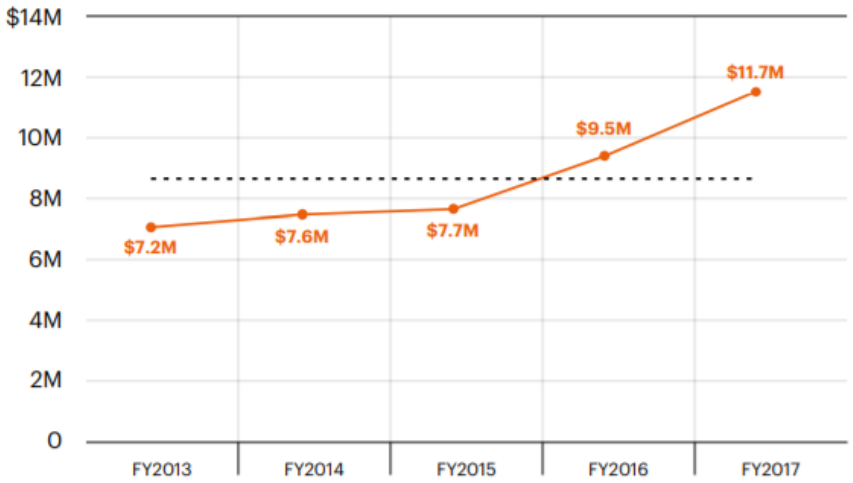


Il·lustració 8. Número d'incidents gestionats pel CCN-CERT. (CCN-CERT, 2017)

4.6. Costos a nivell mundial dels ciberatacs

Segons un estudi realitzat per (Kaspersky Lab, 2017), als Estats Units, el cost resultat d'una filtració d'informació l'any 2017 per grans empreses, de mitjana, és d'$1.3 milions. Pel que fa a les petites i mitjanes empreses, el cost pot arribar als 117.000$. Aquest s'ha incrementat un 11% respecte a anys anteriors.

(Ponemon Institute LLC; Accenture, 2017) A nivell mundial, un estudi que ha fet Ponemon juntament amb Accenture i ha tingut en compte 254 empreses de tot el món, es mostra que el cost, de mitjana, conseqüència d'un ciberatac s'ha incrementat un 62 % durant aquests últims anys, passant dels 7.2 milions de dòlars als 11,7 milions. A sota es mostra la gràfica amb l'evolució (remarcar que les quantitats estan en dòlars americans). La línia discontínua mostraria la mitjana dels últims 5 anys.



Il·lustració 9. Mitjana mundial del cost dels ciberatacs en els últims 5 anys. (Ponemon Institute LLC; Accenture, 2017)

(UE, 2018) Aproximadament, es calcula que a nivell global, l'economia pateix una pèrdua de 400000 milions de dòlars cada any per causa dels ciberatacs. Aquests números han situat la ciberseguretat en el focus de totes les empreses, que busquen protegir-se de les possibles filtracions de dades i tot tipus d'atacs cibernètics.

4.7. Inversió mundial de les empreses en ciberseguretat

Com a conseqüència del punt 4.6, les empreses estan incrementant cada vegada més els pressupostos dedicats a la ciberseguretat. En concret, segons un estudi realitzat per Gartner, Inc (Van der Meulen & Pettey, 2017) es preveu que aquest 2018 s'incrementi en un 8% el pressupost. El principal factor d'aquest increment és per intentar evitar les fugues d'informació, però també entren en joc altres actors com:

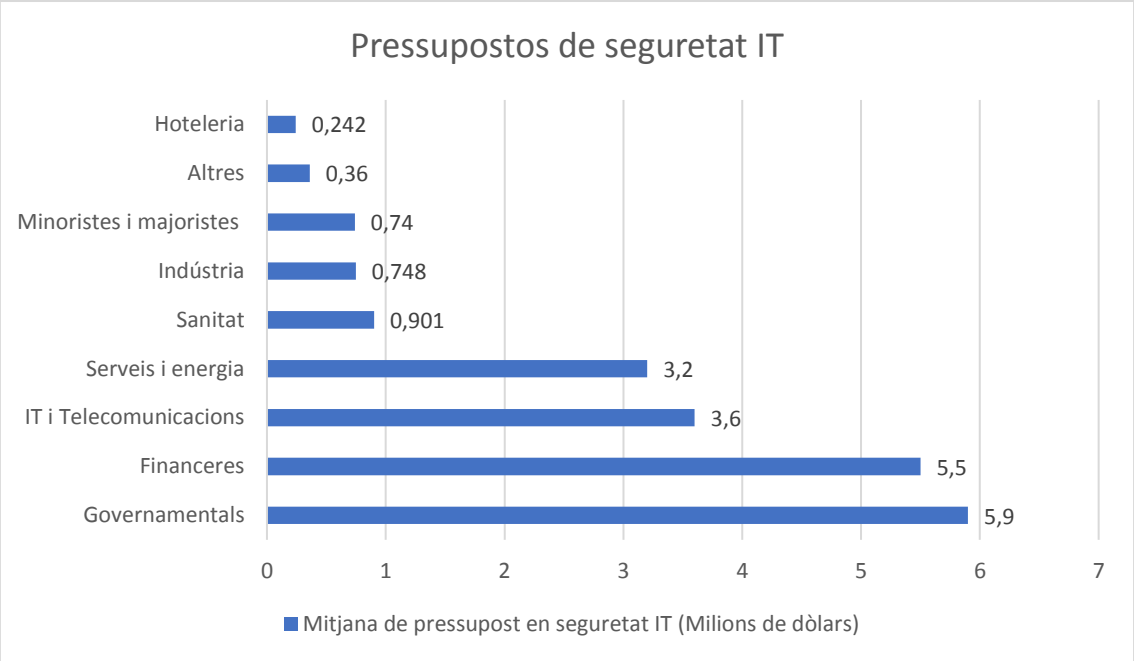
- el compliment de les normatives vigents *(Health Insurance Portability and Accountability Act, National Institute of Standards and Technology, Overseas Citizenship of India* i *General Data Protection Regulation*, entre d'altres) i
- la privacitat de dades.

L'evolució dels pressupostos és la següent:

Taula 4. Evolució de la despesa mundial en seguretat. (Van der Meulen & Pettey, 2017)

	2016	2017	2018
Despesa mundial en seguretat (milions de dòlars actuals)	82,225	89,133	96,296

Les empreses que més inverteixen en seguretat IT són les governamentals, seguides de les financeres i les d'IT i telecomunicacions. El rànquing és el següent:



Il·lustració 10. Pressupostos de seguretat IT segons les companyies. (Ponemon Institute LLC; Accenture, 2017).

4.8. Organismes governamentals de ciberseguretat

Com a conseqüència de la importància de la ciberseguretat en la nostra societat, a partir del segle XXI van anar apareixent diferents organismes governamentals a nivell nacional i internacional.

((ITU) & Minges, 2017) Destacar que segons el GCI (Global Cybersecurity Index), estudi que mesura el compromís i sensibilització a nivell de ciberseguretat dels diferents països membres de les nacions unides (193), la meitat de països tenen una estratègia de ciberseguretat definida. Els 10 països més avançats en aquest sentit són, per ordre: Singapore, Estats Units, Malaysia, Oman, Estònia, Mauritius, Austràlia, Georgia, França i Canadà. Espanya ocupa la posició 54 i està en procés de maduresa d'aquesta estratègia.

A continuació descriurem els que hem considerat més importants (per proximitat o per incidència al món):

Catalunya

(Generalitat de Catalunya, 2018) A Catalunya, existeix el **CESICAT** (Centre de Seguretat de la Informació de Catalunya), creat l'any 2009 amb l'objectiu de ser l'organisme encarregat de garantir la protecció, prevenció i govern en matèria de ciberseguretat de la Generalitat de Catalunya i el seu govern.

(Generalitat de Catalunya, 2018) Addicionalment, el dia 12 de juliol de 2017 es va aprovar al ple del Parlament la creació de **l'Agència de Ciberseguretat de Catalunya**, òrgan que eventualment substituirà el CESICAT. Aquesta s'encarregarà de prevenir, detectar, respondre i investigar incidents o amenaces a les xarxes de comunicacions electròniques i als sistemes d'informació públics, a més de planificar, gestionar, coordinar i supervisar la ciberseguretat de Catalunya. L'objectiu serà minimitzar els danys i els temps de recuperació de les xarxes i els sistemes en cas de ciberatac i col·laborar amb els cossos policials i les autoritats judicials.

Destacar que l'Agència es troba actualment suspesa cautelarment pel tribunal constitucional.

Espanya

A espanya no existeix una agència específica de ciberseguretat, però sí que existeix el **CCN-CERT.** (CCN-CERT, 2018) Aquest forma part del CCN (centre criptològic nacional) i és la línia que té capacitat de resposta a incidents de seguretat de la Informació. Aquest servei es va crear l'any 2006 i entre les seves competències en destaca la gestió dels ciberincidents que afectin a sistemes del sector públic, empreses i organitzacions d'interès estratègic pel país i/o a qualsevol sistema classificat.

La seva missió, doncs, és contribuir en la millora de la ciberseguretat espanyola, sent el centre d'alerta i resposta nacional que coopera i ajuda a respondre de forma ràpida i eficient als ciberatacs i a afrontar de forma activa les ciberamenaces. El CERT està operat per INCIBE.

(INCIBE, 2018) L**'INCIBE** (Institut Nacional de Ciberseguretat d'Espanya), és una societat que depèn del Ministeri d'Energia, Turisme y Agenda Digital. Es tracta d'un instrument del govern per reforçar la ciberseguretat, la confiança i la protecció de la informació i privacitat en els serveis de la Seguretat de la informació, aportant valor als ciutadans, empreses, administració, xarxa acadèmica i d'investigació espanyola, el sector de les tecnologies de la informació i les comunicacions i sector estratègics en general.

Europa

A nivell europeu existeix l'**ENISA** (European Union Agency for Network and Information Security) (ENISA, 2018), creat l'any 2004 i ubicat a Grècia, és el centre de coneixement de ciberseguretat a Europa. El seu objectiu és contribuir a la securització a nivell europeu de la informació mitjançant la sensibilització sobre la seguretat de la xarxa i la informació, així com desenvolupar i promoure una cultura en benefici dels ciutadans, consumidors, empreses i organitzacions del sector públic en la unió.

(UE, 2018) A més, els dies 19 i 20 d'Octubre de 2017, la unió europea, per tal de reforçar les normes sobre ciberseguretat i fer front a la creixent amenaça que representen els atac cibernètics, va proposar un seguit de reformes que presenten com a principals iniciatives:

- La creació d'una agència de ciberseguretat de la UE més forta, en base a l'ENISA.
- La introducció d'un règim de certificació de la ciberseguretat a escala de la UE (CERT-UE).
- La ràpida aplicació de la directiva NIS (Network Information Security).

El **CERT-UE**, creat el 20 de desembre de 2017, és un equip de resposta a emergències informàtiques de caràcter permanent que cobreix totes les institucions, òrgans i organismes de la UE. Aquest assegurarà una resposta coordinada de la UE enfront als ciberatacs dirigits contra les seves institucions.

Estats Units

(NSA | CSS, 2018) Els estats units van ser dels pioners en aquest sector. L'any 1952 van crear l' **NSA** (agència de seguretat nacional), que ha anat evolucionant i adaptant-se a les noves tecnologies. Actualment la NSA és responsable de la monitorització, recol·lecció i processat d'informació i dades amb finalitats d'intel·ligència i contraespionatge. A més també té com a missió la protecció de les xarxes de comunicacions i els sistemes d'informació dels estats units.

4.9. Directives / lleis que fan referència a la ciberseguretat

4.9.1. Directives nacionals

Esquema nacional de Seguridad (ENS)

(CCN-CERT, 2018) La llei 11/2007, del 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics va establir l'Esquema Nacional de Seguretat que, aprovat el 8 de gener de 2010 té com a objectiu determinar la política de seguretat en la utilització de mitjans electrònics en el seu àmbit d'aplicació i està constituït pels principis bàsics i requeriments mínims que permeten una protecció adequada de la informació.

L'ENS assenyala que els sistemes d'informació als quals fa referència seran objecte d'auditoria regular ordinària almenys cada dos anys.

4.9.2. Directives europees

Directiva NIS (Network Information Security)

(UE, 2016) La directiva NIS estableix mesures amb l'objectiu d'aconseguir un elevat nivell comú de seguretat de les xarxes i els sistemes d'informació dins la unió europea a fi de millorar el funcionament del mercat interior.

Amb aquest fi,

- estableix obligacions per tots els estats membres d'adoptar una estratègia nacional de seguretat de les xarxes i sistemes d'informació.
- crea un grup de cooperació per recolzar i facilitar la cooperació estratègica i l'intercanvi d'informació entre els estats membres.
- crea una xarxa d'equips de resposta a incidents de seguretat informàtica (CSIRT – Computer Security Incident Response Team) amb la finalitat de contribuir al desenvolupament de la confiança i la seguretat entre els estats membres i promoure una cooperació operativa ràpida i eficaç.
- estableix requeriments en matèria de seguretat i notificacions pels operadors de serveis essencials o proveïdors de serveis digitals.
- estableix obligacions perquè els estats membres designin autoritats nacionals competents, punts de contacte únics i CSIRT amb funcions relacionades amb la seguretat de les xarxes i els sistemes d'informació.

Destacar que els requeriments de seguretat d'aquesta directiva no seran aplicables a les empreses que estan subjectes als requeriments dels articles 13 bis i 13 ter de la Directiva 2002/21/CE.

4.10. Organismes reguladors existents

4.10.1. Organismes internacionals

(Lázaro Anguís, 2017) En l'àmbit internacional, existeixen dos organismes de normalització:

- **IEC** (International Electrotechnical Comission), responsable de l'elaboració de normes internacionals sobre electrotècnia i electrònica.
- **ISO** (International Organization for Standardization), que cobreix la resta de sectors d'activitat. Es tracta d'una organització no governamental mundial, fundada el 1947 amb seu a Ginebra i que representa a 170 països.

Aquests dos organismes comparteixen la responsabilitat d'elaborar las normes relatives a les tecnologies de la informació.

4.10.2. Organismes europeus

En l'àmbit europeu, existeixen tres organismes de normalització reconeguts. Només els estàndards desenvolupats per les tres ESO (European Standards Organization) són reconeguts a nivell europeu.

- **CEN** (European Committee for Standardization)
  (CEN | CENELEC, 2018) Fundada el 1961, és una organització sense ànim de lucre, basada a Brussel·les, que té com a objectiu desenvolupar i mantenir normatives que millorin l'economia de la unió europea.
- **CENELEC** (European Committee for Electrotechnical Standardization)
  (CEN | CENELEC, 2018) Fundada el 1973, és una organització sense ànim de lucre, basada a Brussel·les, que té com a objectiu normalitzar les normatives dins l'àrea de l'enginyeria elèctrica.
- **ETSI** (European Telecommunications Standards Institute)
  (ETSI, 2018) Fundada el 1988, és una organització sense ànim de lucre, basada a França, que té per objectiu l'estandardització de la indústria de les telecomunicacions (fabricants d'equips i operadors de xarxes) d'Europa, tot i tenir una clara projecció a nivell mundial.

4.10.3. Organismes nacionals

(AENOR, 2018) En l'àmbit de l'estat espanyol, existeix la **AENOR** (Asociación Española de Normalización y Certificación), fundada l'any 1986, que és l'associació privada sense ànim de lucre que desenvolupa l'activitat de normalització (mitjançant les normes UNE) i cooperació dels diferents àmbits, entre els quals es troba la tecnologia de la informació.

És l'organització que representa a Espanya davant dels organisme europeus i internacionals.

4.11. Reglaments de protecció de dades de caràcter personal

Com ja hem comentat, la seguretat de la informació protegeix tota aquella informació considerada sensible perquè no sigui accedida per personal no autoritzat. Una part molt important d'aquesta informació és el que anomenem les dades de caràcter personal.

(Boletín Oficial del estado, 2018) Considerarem per dades de caràcter personal qualsevol tipus d'informació (numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus) relativa a persones físiques identificades o identificables ("l'interessat"). Es considera persona física identificable tota persona la identitat de la qual pugui determinar-se, directa o indirectament.

Exemples de dades de caràcter personal serien: nom, cognom, data de naixement, correu electrònic, DNI/NIF, dades biomètriques, dades genètiques, fotografia, número de la seguretat social, estat civil, etc.

També hi ha categories especials de dades personals com ara: origen ètnic o racial, opinions polítiques, conviccions religioses o filosòfiques, ideologia, afiliació sindical, dades de salud, dades d'orientació sexual.

Per aquest treball, només es tindran en compte aquells reglaments que apliquen a nivell de l'estat espanyol. (Reglament, 2018) Entenent per reglament tot aquell conjunt de regles i disposicions a seguir o complir en l'execució d'una llei, per al règim d'una societat, una dependència, etc. I que, per tant, són d'obligat compliment.

Fins aquest any, a Espanya només aplicava la LOPD (Ley Orgánica de Protección de Datos). Amb l'entrada en vigor de la GDPR (General Data Protection Regulation) també cal tenir-la en compte ja que és un reglament d'aplicació directa. És a dir, els preceptes de la GDPR seran d'aplicació directa a l'ordenament jurídic espanyol sense necessitat de transposició, per la qual cosa, en principi coexistirà amb la LOPD mentre no es contradigui amb el que es disposa a la normativa europea.

A continuació es farà un breu resum de cada un dels reglaments:

4.11.1. LOPD (Ley Orgánica de Protección de datos)

(Boletín Oficial del estado, 2018) Es va publicar el 14 de desembre de 1999 i entrà en vigor el 14 de gener del 2000. La LOPD té per objectiu garantir i protegir, en el que fa referència al tractament de les dades personals, llibertats públiques i drets fonamentals de les persones físiques, especialment del seu honor i intimitat personal i familiar.

4.11.2. GDPR (General Data Protection Regulation)

(Hechkh, 2018) El 25 de gener de 2012 es va redactar el primer esborrany de la GDPR, però no va ser fins el 14 d'abril del 2016 que fou aprovada pel Parlament europeu. Aquesta entrà en vigor i és d'obligat compliment des del 25 de maig de 2018.

La GDPR

- estableix les normes relatives a la protecció de les persones físiques en el que fa referència al tractament de les dades personals i les normes relatives a la lliure circulació d'aquestes.
- protegeix els drets i llibertats fonamentals de les persones físiques i, en particular, el seu dret a la protecció de les dades personals.

L'aplicació de la GDPR a nivell europeu suposa poder:

- Garantir un nivell uniforme i elevat de protecció de les persones físiques.
- Eliminar obstacles a la circulació de dades personals.
- Proporcionar seguretat jurídica i transparència als operadors jurídics.
- Aconseguir el mateix nivell de drets i obligacions de les persones físiques de tots els estats membres.
- Establir un mateix nivell de responsabilitats en tots els estats membres.

4.11.3. Principals novetats de la GDPR versus la LOPD

(APDCAT. Autoritat Catalana de Protecció de Dades, 2018) A continuació destacarem les principals novetats d'aquest nou reglament europeu:

- **Àmbit d'aplicació**: El Reglament amplia l'àmbit d'aplicació territorial als responsables i als encarregats del tractament no establerts a la UE, quan les activitats de tractament estan relacionades amb l'oferta de béns o serveis o amb el control del comportament de les persones, si tenen lloc a la UE.
- **Principis**
  - Responsabilitat proactiva: requereix que les organitzacions analitzin quines dades tracten, amb quines finalitats ho fan i quin tipus d'operacions de tractament duen a terme. A partir d'aquest coneixement, han de determinar de manera explícita com aplicaran les mesures que preveu la GDPR. Així mateix, s'han d'assegurar que aquestes mesures són les adequades per complir-lo i que

poden demostrar-ne el compliment davant les persones interessades i davant les autoritats de supervisió.

En síntesi, aquest principi exigeix que les organitzacions tinguin una actitud conscient, diligent i proactiva davant de tots els tractaments de dades personals que duguin a terme.

- Enfocament de risc: La GDPR assenyala que les mesures adreçades a garantir-ne el compliment han de tenir en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, així com el risc per als drets i les llibertats de les persones.

  D'acord amb aquest enfocament, algunes de les mesures que la GDPR estableix només s'han d'aplicar quan hi hagi un alt risc per als drets i les llibertats, mentre que d'altres s'han de modular d'acord amb el nivell i tipus de risc que presentin els tractaments.

- **Noves categories especials de dades**: dades genètiques i dades biomètriques.
- **Consentiment**: La GDPR requereix que l'interessat presti el consentiment mitjançant una declaració inequívoca o una acció afirmativa clara. Als efectes del nou Reglament, les caselles ja marcades, el consentiment tàcit o la inacció no constitueixen un consentiment vàlid.
- **Consentiment dels menors**: En l'àmbit dels serveis de la societat de la informació, el consentiment dels menors només és vàlid si tenen més de 16 anys. No obstant això, els estats membres de la UE poden rebaixar l'edat fins als 13 anys.
- **Dret d'informació:** El nou Reglament configura la informació com un dret de les persones afectades i amplia les qüestions sobre les quals cal informar-les, amb els aspectes següents: les dades de contacte del delegat de protecció de dades; la base jurídica del tractament; els interessos legítims perseguits en què es fonamenta el tractament, si escau; la intenció de transferir les dades a un tercer país o a una organització internacional i la base per fer-ho, si escau; el termini durant el qual es conservaran les dades; el dret a sol·licitar la portabilitat; el dret a retirar en qualsevol moment el consentiment que s'hagi prestat; si la comunicació de dades és un requisit legal o contractual o un requisit necessari per subscriure un contracte; el dret a presentar una reclamació davant una autoritat de control; l'existència de decisions automatitzades, inclosa la lògica aplicada i les seves conseqüències.
- **Drets de les persones interessades**: La GDPR incorpora el dret a l'oblit com un dret vinculat al dret de supressió, al dret a la limitació del tractament i al dret a la portabilitat.
- **Inscripció i notificació de fitxers:** La GDPR suprimeix, a partir del 25 de maig de 2018, la necessitat de crear formalment els fitxers i notificar-los al registre de protecció de dades de les autoritats de control.
- **Documentació de les operacions de tractament: registre d'activitats de tractament.** LA GDPR preveu noves obligacions de documentació del tractament per als responsables o els encarregats del tractament.
- **Encàrrec del tractament:** El Reglament amplia el contingut mínim del contracte d'encàrrec de tractament. Entre altres aspectes, el contracte ha de preveure els punts addicionals següents respecte del contingut que ja establia la LOPD: l'objecte i la durada de l'encàrrec; la naturalesa del tractament; el tipus de dades personals; les categories d'interessats; les obligacions i els drets del responsable; la previsió que les persones que han de tractar les dades es comprometen a mantenir la confidencialitat; l'assistència de l'encarregat al responsable per atendre les sol·licituds d'exercici de

drets; la supressió o la devolució de les dades en finalitzar l'encàrrec; l'obligació de posar a disposició del responsable tota la informació necessària per demostrar que compleix les obligacions de l'encarregat del tractament i per permetre i contribuir que el responsable o un altre auditor autoritzat pel responsable efectuï auditories i inspeccions.

- **Avaluacions d'impacte relatives a la protecció de dades:** Quan sigui probable que un tractament suposi un risc alt per als drets i les llibertats de les persones físiques, per la seva naturalesa, abast, context o finalitats, especialment si s'utilitzen les noves tecnologies, abans d'iniciar el tractament el responsable ha de fer una avaluació de l'impacte de les operacions de tractament en la protecció de dades personals.
- **Consulta prèvia:** Si de l'avaluació d'impacte sobre la protecció de dades en resulta que el tractament previst pot infringir la GDPR, en particular quan el responsable no ha identificat o mitigat suficientment el risc, el responsable ha de fer una consulta a l'autoritat de control de protecció de dades competent.

  En els casos en què les avaluacions d'impacte identifiquin un alt risc que, a parer del responsable de tractament, no es pugui mitigar per mitjans raonables en termes de tecnologia disponible i costos d'aplicació, el responsable ha de consultar l'autoritat de protecció de dades competent. La consulta ha d'anar acompanyada de la documentació que preveu la GDPR, inclosa la mateixa avaluació d'impacte.

  L'autoritat de control ha d'assessorar per escrit el responsable i, si escau, l'encarregat, i pot fer ús de tots els poders que li confereix el Reglament, entre els quals hi ha prohibir l'operació de tractament.
- **Protecció de dades des del disseny i per defecte:** El Reglament introdueix els conceptes de privacitat des del disseny i privacitat per defecte.

  Això implica que el responsable ha d'aplicar, tant en el moment de determinar els mitjans de tractament com en el moment del tractament mateix, les mesures tècniques i organitzatives adequades concebudes per aplicar de manera efectiva els principis de protecció de dades (com, per exemple, la pseudonimització), i integrar les garanties necessàries en el tractament per complir els requeriments del Reglament.

  Així mateix, el responsable ha d'aplicar les mesures tècniques i organitzatives adequades per garantir que, per defecte, només es tracten les dades personals necessàries per a cada finalitat específica del tractament.
- **Codis de conducta:** La GDPR també regula els codis de conducta que poden promoure les associacions i altres organismes representatius de categories de responsables del tractament o d'encarregats del tractament, perquè el Reglament s'apliqui correctament.

  El codi de conducta s'ha de presentar a l'autoritat de control competent, perquè l'aprovi, la registri i la publiqui. També correspon a l'autoritat de control acreditar l'organisme de supervisió que preveu el codi.

  L'adhesió i el compliment d'un codi de conducta és un element a tenir en compte a l'hora de demostrar que el responsable del tractament compleix les seves obligacions, especialment en el moment de fer l'avaluació d'impacte sobre la protecció de dades.
- **Mecanismes de certificació:** El Reglament també promou els mecanismes de certificació, com certificats, segells o marques, per demostrar que es compleix la GDPR.
- **Delegat de protecció de dades (DPD):** El Reglament introdueix la figura del delegat de protecció de dades, que pot formar part de la plantilla del responsable o l'encarregat o bé actuar en el marc d'un contracte de serveis. Cal designar un delegat de protecció de dades en els casos següents:

  - Quan el tractament el dugui a terme una autoritat o un organisme públic (tret de jutjats i tribunals). En aquest cas, es pot designar un únic delegat de protecció de dades per a diverses d'aquestes autoritats o organismes.
  - Quan el tractament requereix l'observació habitual i sistemàtica d'interessats a gran escala.
  - Quan el tractament té per objecte categories especials de dades personals o dades relatives a condemnes o infraccions penals.

  El delegat de protecció de dades té, entre d'altres, les funcions següents:
  - Informar i assessorar el responsable o l'encarregat i els treballadors sobre les obligacions que imposa la normativa de protecció de dades.
  - Supervisar que es compleix la normativa.
  - Assessorar respecte de l'avaluació d'impacte relativa a la protecció de dades.
  - Cooperar amb l'autoritat de control.
  - Actuar com a punt de contacte per a qüestions relatives al tractament.
- **Transferències internacionals:** es manté igual que amb la LOPD.
- **Mesures de seguretat:** A diferència de la normativa actual, el Reglament no estableix un llistat de les mesures de seguretat que s'han aplicar d'acord amb la tipologia de dades objecte de tractament, sinó que estableix que el responsable i l'encarregat del tractament han d'aplicar les mesures tècniques i organitzatives adequades al risc que comporta el tractament. Això implica que cal fer una avaluació dels riscos associats a cada tractament, per determinar les mesures de seguretat que cal implementar.
- **Notificació de violacions de seguretat**: Si es produeix una violació de la seguretat, el responsable l'ha de notificar a l'autoritat de control en un termini màxim de 72 hores, tret que sigui improbable que constitueixi un risc per als drets i les llibertats de les persones.
- **Finestreta única:** possibilitat de plantejar les reclamacions davant de qualsevol autoritat de control sense necessitat de que aquestes reclamacions es vinculin al lloc de residència del denunciant.

Com es pot veure, aquesta nova normativa promou l'elaboració d'avaluacions d'impacte (PIA - Privacy Impact Assessments) i anàlisis de riscos per avaluar les mesures de seguretat a implementar.

4.11.4. PCI DSS (Payment Card Industry Data Security Standard)

(PCI Security Standards Council, 2018) PCI DSS és un estàndard de seguretat de la informació aplicable a totes les organitzacions que tracten amb dades de targetes de crèdit. La seva prioritat és que les organitzacions entenguin i implementin estàndards que protegeixin els seus sistemes de pagament envers a possibles fugues d'informació o robatori de dades.

Actualment hi ha 12 estàndards que totes les organitzacions haurien de complir. Aquests cobreixen la part tècnica i operacional dels components del sistema inclosos o connectats a dades de targetes de crèdit. A continuació es mostren els 12 estàndards relacionats amb el seu principal objectiu:

Taula 5. Estàndards PCI DSS. (PCI Security Standards Council, 2018)

Objectiu	Estàndard
Construir i mantenir una xarxa segura	• Instal·lar i mantenir una configuració de Firewall per protegir les dades de targetes de crèdit. • No utilitzar contrasenyes per defecte ni altres paràmetres de seguretat per defecte.
Protegir les dades de targetes de crèdit	• Protegir les dades emmagatzemades. • Encriptar la transferència de dades entre xarxes obertes i/o públiques.
Mantenir un programa de gestió de les vulnerabilitats	• Utilitzar i actualitzar de forma periòdica l'anti-virus. • Desenvolupar i mantenir sistemes i aplicacions segurs.
Implementar mesures de control d'accés	• Restringir l'accés a informació de targetes de crèdit agafant com a base la necessitat de l'usuari de conèixer la informació. • Assignar una identificació única a cada persona que tingui accés a un ordinador. • Restringir l'accés físic a les dades dels propietaris de targetes.
Monitoritzar i testejar les xarxes	• Rastrejar i monitoritzar tot accés a recursos de xarxa i a dades dels propietaris de targetes. • Provar regularment els sistemes i processos de seguretat.
Mantenir polítiques de seguretat de la informació	• Mantenir una política que contempli la seguretat de la informació.

4.12. Marcs de control existents

A continuació citarem un conjunt de normes i estàndards que són d'aplicació voluntària però que descriuen un conjunt de bones pràctiques a seguir per garantir un nivell de seguretat de la informació acceptable. Es tracta dels principals estàndards utilitzats pel control intern dins les empreses.

4.12.1. ISO/IEC

ISO/IEC 27000

(Lázaro Anguís, 2017) Publicada l'1 de maig del 2009, revisada amb una segona edició l'1 de desembre del 2012 i una tercera edició el 14 de gener de 2014. Aquesta norma proporciona les directrius del sistema de gestió de la seguretat de la informació (SGSI o ISMS en anglès) i del vocabulari.

UNE-ISO/IEC 27001:2014

(Lázaro Anguís, 2017) Publicada el 15 d'Octubre de 2005, revisada el 25 de setembre de 2013. És la norma principal de la sèrie i conté els requisits del sistema de gestió de seguretat de la informació. En el seu Annex A, enumera en forma de resum els objectius de control i controls que desenvolupa la ISO 27002:2005, perquè siguin seleccionats per les organitzacions en el desenvolupament dels seus SGSI; tot i no ser obligada la implementació de tots els controls

enumerats en l'annex, l'organització haurà d'argumentar sòlidament la no aplicabilitat dels controls no implementats.

ISO/IEC 27002:2013

(Lázaro Anguís, 2017) Es una guia de bones pràctiques que descriu els objectius de control i controls recomanats a nivell de seguretat de la informació. No es certificable.

4.12.2. Cobit (Control Objectives for Information Systems and related Technology)

(Lázaro Anguís, 2017) És un model d'avaluació i monitorització que posa èmfasis en el control dels negocis i la seguretat IT. Ha estat desenvolupat per experts de l'associació d'auditor de sistemes d'informació (ISACA) i descriu controls específics TI des d'una perspectiva de negoci.

Defineix un marc de referència que classifica els processos de les unitats de tecnologia de la informació de les organitzacions en quatre dominis principals:

- Planificació i Organització.
- Adquisició i implantació.
- Suport i Serveis.
- Monitorització.

4.12.3. NIST Cybersecurity framework for Critical Infrastructure Protection

(NIST, 2018) És un marc de controls que consisteix amb un seguit d'estàndards, directrius i bones pràctiques per gestionar el risc de ciberseguretat. Ha estat desenvolupat per l'Institut Nacional de Normes i Tecnologia (National Institute of Standards and Technology), als estats units.

Aquest marc de controls ajuda a promoure la protecció i resiliència de la infraestructura crítica i altres sectors importants de l'economia i la seguretat nacional.

(ISACA, 2017) Identifica 5 accions clau per la protecció dels actius digitals. Aquestes accions coincideixen amb els mètodes definits per la gestió d'incidents i inclouen:

Taula 6. Funcions principals del marc de controls de ciberseguretat de NIST.

Funcions	Descripció
IDENTIFICAR	Utilitzar el coneixement d'una organització per minimitzar el risc en els sistemes, actius, informació i competències.
PROTEGIR	Dissenyar proteccions per limitar l'impacte de potencials esdeveniments en serveis o infraestructures crítiques.
DETECTAR	Implementar activitats per identificar l'ocurrència d'un esdeveniment de ciberseguretat.
RESPONDRE	Prendre les mesures adequades després de que s'esdevinguin un esdeveniment de seguretat.
RECUPERAR	Pla de recuperació dins del temps adequat de les capacitats i serveis compromesos.

Dins d'aquestes funcions es defineixen 23 dominis que donaran lloc a 108 objectius de control.

Taula 7. Relació entre funcions i dominis del marc de controls de ciberseguretat de NIST.

Funcions	Dominis	Núm. de controls
IDENTIFICAR (29 controls associats)	Gestió d'actius	6
	Entorn de negoci	5
	Govern	4
	Anàlisi de riscos	6
	Estratègia de gestió del risc	3
	Gestió del risc de la cadena de subministrament	5
PROTEGIR (39 controls associats)	Gestió d'identitats, autenticació i control d'accés	7
	Sensibilització i formació	5
	Seguretat de les dades	8
	Processos i procediments de protecció de la informació	12
	Manteniment	2
	Protecció de la tecnologia	5
DETECTAR (18 controls associats)	Anomalies i esdeveniments	5
	Monitorització contínua de la seguretat	8
	Processos de detecció	5
RESPONDRE (16 controls associats)	Planificació de la resposta a incidents	1
	Comunicacions	5
	Anàlisi	5
	Mitigació	3
	Millores	2
RECUPERAR (6 controls associats)	Planificació de la recuperació	1
	Comunicacions	2
	Millores	3

4.13. Cloud computing

Aquest apartat té com objectiu introduir els conceptes bàsics de cloud computing i donar una visió de com està el mercat actualment. (ENISA, 2009) Comentar que el cloud computing és una nova manera d'oferir recursos informàtics no una nova tecnologia.

Per evitar errors de comprensió, destacar que al llarg del document farem referència als següents termes:

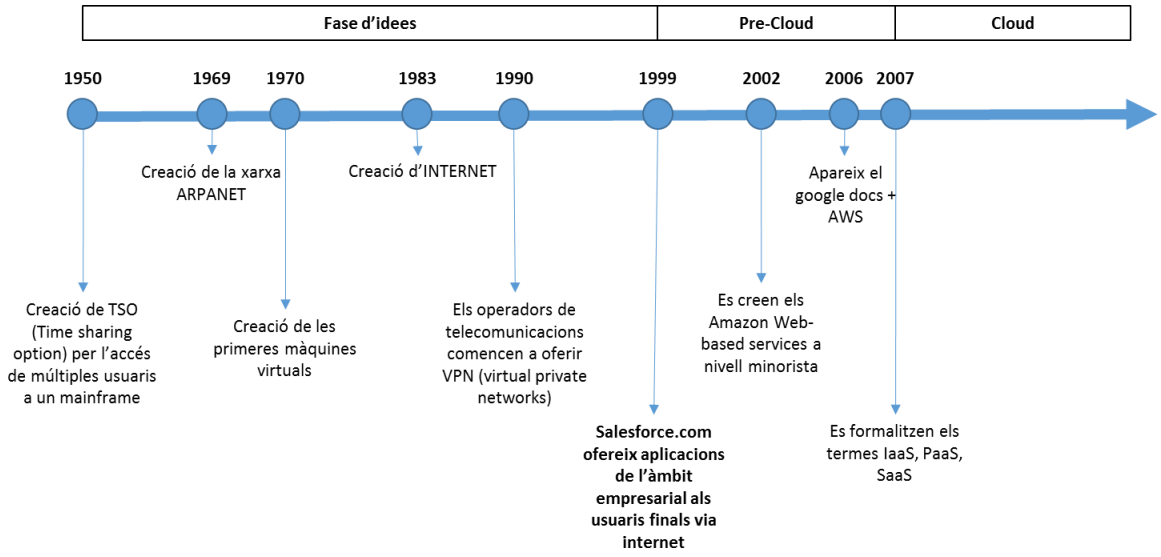
- **Usuari o client dels serveis cloud**: persona o organització que és client d'un servei cloud. Destacar que un client cloud també por ser un cloud ell mateix ja que els clouds s'ofereixen serveis entre ells.
- **Client cloud**: una màquina o software d'aplicació que accedeix el cloud sobre una connexió de xarxa en nom d'un usuari.
- **Proveïdor de serveis cloud**: organització que proporciona serveis cloud als usuaris.

4.13.1. Evolució

Es dividirà l'evolució del cloud en tres fases: etapa d'idees (1950 – 1999), fase pre-cloud (1999 – 2006) i fase cloud (2006 – Actualitat).

- **Etapa d'idees (1950 – 1999)**
  (Destefani Neto, 2014) Es podria dir que tot va començar durant la dècada dels 50 amb la creació dels TSO (Time Sharing Options), que permetien l'accés de múltiples usuaris a la vegada a un ordinador central.
  (Foote, 2017) Posteriorment, l'any 1969 es va crear l'Arpanet, una versió primitiva de l'Internet. Un dels seus creadors, JCR Licklider, volia que allò evolucionés cap a el que ell anomenava una Xarxa d'Ordinadors Intergalàctica, que pretenia interconnectar a tot el planeta mitjançant ordinadors i així poder accedir a la informació des d'on fos. D'aquí va néixer doncs, la idea d'Internet que seria l'eina necessària per poder accedir al cloud.
  L'any 1970 es van crear les primeres màquines virtuals, que permetien executar diferents sistemes operatius / programes alhora en una sola infraestructura.
  Als anys 90, es va començar a utilitzar el terme cloud per expressar l'espai que hi havia entre l'usuari final i el proveïdor quan les companyies de telecomunicacions van començar a oferir xarxes virtuals privades (VPN). Aquestes tenien les mateixes qualitats de servei que les xarxes punt a punt, però permetien als proveïdors de telecomunicacions re-utilitzar la infraestructura i, en conseqüència, reduir costos.
- **Fase pre-cloud (1999 – 2006)**
  (Foote, 2017) L'any 1999 es produeix una de les fites més importants quan Salesforce.com treu al mercat una aplicació de l'àmbit empresarial que pot ser utilitzada per l'usuari final via Internet. Van ser els primers a utilitzar l'Internet per oferir programes software als usuaris (SaaS).
  Posteriorment, l'any 2002 Amazon va començar a oferir als clients finals serveis basats en web.
- **Fase cloud (2006 – Actualitat)**
  (Foote, 2017) Un cop els proveïdors de telecomunicacions van començar a oferir un ample de banda considerable, podríem dir que neix el que coneixem avui en dia com a cloud computing. L'any 2006, per exemple, van aparèixer els famosos Amazon Web Services i Google Docs services. A partir d'aleshores, els proveïdors de cloud no han parat d'oferir serveis nous a les empreses basats ens els conceptes de Iaas, SaaS i PaaS.

A continuació es mostra un gràfic amb les principals fites de l'evolució del cloud computing:



Il·lustració 11. Evolució del cloud computing.

4.13.2. Principals amenaces dels serveis de cloud computing

Anteriorment, en el punt 4.4, es donava la foto actual de les principals amenaces de ciberseguretat. Ja que el treball se centra en la implementació de serveis utilitzant el cloud computing, en aquest punt, el que es pretén és donar la visió d'amenaces específiques pel cloud juntament amb l'impacte d'aquestes i els seus controls mitigants. Aquesta informació s'utilitzarà posteriorment per poder realitzar l'anàlisi de riscos.

(CSA, 2017) A continuació, doncs, es mostren les principals amenaces de seguretat que afecten als serveis de cloud computing, així com:

- Els riscos addicionals envers un entorn no cloud.
- Els controls mitigants proposats per preveure i gestionar aquestes amenaces. Destacar que s'ha utilitzat la nomenclatura dels controls inclosos en el marc de controls CSA-CCM perquè després sigui més fàcil fer-ne la correspondència (amenaça vs control) a l'hora de realitzar l'anàlisi de riscos. (CSA, 2017).
- L'impacte de cadascuna d'aquestes amenaces. S'utilitzarà posteriorment pel càlcul del risc inherent.
- I la correspondència d'aquestes amb les principals amenaces de ciberseguretat.

Taula 8. Principals amenaces cloud computing. (CSA, 2017)

Núm.	Amenaces cloud computing	Riscos addicionals	Controls mitigants
1 **(11*)**	**Fuga d'informació**	- Recursos de xarxa compartits. - Personal del proveïdor de cloud i els seus dispositius. - Tercers contractats pel proveïdor de cloud. - Quantitat de dades disponibles al cloud de forma centralitzada. Destacar que els proveïdors de cloud tenen seguretat desplegada per tot allò que consideren que és responsabilitat seva, però són els clients qui són responsables de protegir les seves dades dins del cloud.	Els controls més destacats per aquest cas serien: - Multi-factor d'autenticació. - Encriptació de les dades. Controls mitigants a implementar segons CSA-CCM: *AIS-04, CCC-02, DSI-02, DSI-05, DSI-06, DSI-08, EKM-02, EKM-03, EKM-04, GRM-02, GRM-10, HRS-02, HRS-06, IAM-02, IAM-04, IAM-05, IAM-07, IAM-09, IAM-12, IVS-08, IVS-09, IVS-11, SEF-03, STA-06.*
2	**Pobre gestió d'identitats, credencials i accessos**	- Federació d'identitats amb el proveïdor cloud (p.e. SAML). - Centralització dels sistemes d'emmagatzemat de dades crítiques (contrasenyes, claus privades, ...).	Els controls més destacats per aquest cas serien: - Multi-factor d'autenticació. - Establir una política de contrasenyes correcta. - Canvi automàtic i periòdic de claus criptogràfiques, contrasenyes i certificats. - Ús de PKI per evitar l'exposició pública de credencials i claus criptogràfiques. - Implementació de sistemes de gestió d'identitats. Controls mitigants a implementar segons CSA-CCM: *IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, HRS-01, HRS-03, HRS-04, HRS-08, HRS-09, HRS-10*

Núm.	Amenaces cloud computing	Riscos addicionals	Controls mitigants
3 **(2,3)***	**APIs no segures**	- Exposició d'interfícies d'usuaris (UI) o interfícies de programa d'aplicació (APIs) que els clients utilitzen per interactuar amb els serveis cloud i realitzar l'aprovisionament, la gestió, les operacions i la monitorització dels seus sistemes. - Compartició de credencials amb tercers per part dels usuaris de cloud, degut a l'existència d'una doble capa d'APIs, ja que les organitzacions construeixen els seus serveis sobre les APIs existents dels proveïdors cloud.	Els controls més destacats per aquest cas serien: - Control d'accés i autenticació. - Encriptació de dades. - Monitorització d'activitats. - Anàlisi de la securització de les APIs proporcionada pel proveïdor de cloud mitjançant la creació de models de fluxes d'informació, d'arquitectura / disseny, la revisió de codi i pen-testing. Controls mitigants a implementar segons CSA-CCM: *AIS-01, AIS-04, IAM-08, IAM-09*
4	**Vulnerabilitats de sistema i aplicació**	- Amb l'aparició dels multi-tenants i el cloud computing, els sistemes de diverses organitzacions es troben "a prop", compartint memòria, recursos, infraestructura, etc...	Els controls més destacats per aquest cas serien: - Escanejos periòdics de vulnerabilitats. - Instal·lació de patches dels sistemes i actualitzacions. - Dissenys i arquitectures segures. - Processos de gestió del canvi. Controls mitigants a implementar segons CSA-CCM: *AIS-01, AIS-02, AIS-03, AIS-04, BCR-04, CCC-03, IVS-05, IVS-07, TVM-02*
5 **(12)***	**Apropiació indeguda de comptes**	- Si un atacant té accés a les credencials d'un client de cloud, pot utilitzar el compte per redirigir certs clients cap a altres serveis i perpetrar l'atac.	Els controls més destacats per aquest cas serien: - Definició d'una política de passwords correcta. - Gestió de credencials. - Estratègies de Defense-in-depth. - Doble factor d'autenticació. Controls mitigants a implementar segons CSA-CCM: *IAM-02, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IVS-01, SEF-02*

Núm.	Amenaces cloud computing	Riscos addicionals	Controls mitigants
6 **(9)***	**Atacants interns maliciosos**	- Apareix una altra capa d'atacants interns, els que gestionen els sistemes dels proveïdors cloud, tot i que s'implementi una segregació de funcions perquè els responsables de la gestió de claus no tinguin accés a l'administració de dades emmagatzemades.	Els controls més destacats per aquest cas serien: - Encriptació. - Segregació de funcions. - Processos d'auditoria del proveïdor de cloud. - Monitorització mitjançant logs de les activitats dels administradors. Controls mitigants a implementar segons CSA-CCM: *DCS-04, DCS-08, DCS-09, DSI-04, DSI-06, EKM-02, EKM-03, GRM-07, GRM-10, HRS-02, HRS-07, IAM-05, IAM-01, IAM-08, IAM-09, IAM-10, IVS-09, STA-09*
7	**Advanced Persistent Threats (APTs)**	- Quantitat de dades sensibles disponibles al cloud de forma centralitzada.	Els controls més destacats per aquest cas serien: - Gestió de processos. - Plans de resposta d'incidents. - Formació del personal IT. Controls mitigants a implementar segons CSA-CCM: *AIS-01, AIS-02, AIS-03, AIS-04, BCR-04, IVS-01, IVS-02, IVS-05, IVS-07, IVS-13, TVM-01, TVM-02*
8	**Pèrdua d'informació**	- El proveïdor de serveis cloud pot esborrar accidentalment les dades. - Desastres naturals que afectin a molts clients degut a la centralització dels serveis cloud.	Els controls més destacats per aquest cas serien: - Back-up. - Disaster Recovery test. - Plans de continuïtat de negoci. - Redundància geogràfica. Controls mitigants a implementar segons CSA-CCM: *BCR-04, BCR-05, BCR-06, GRM-02*

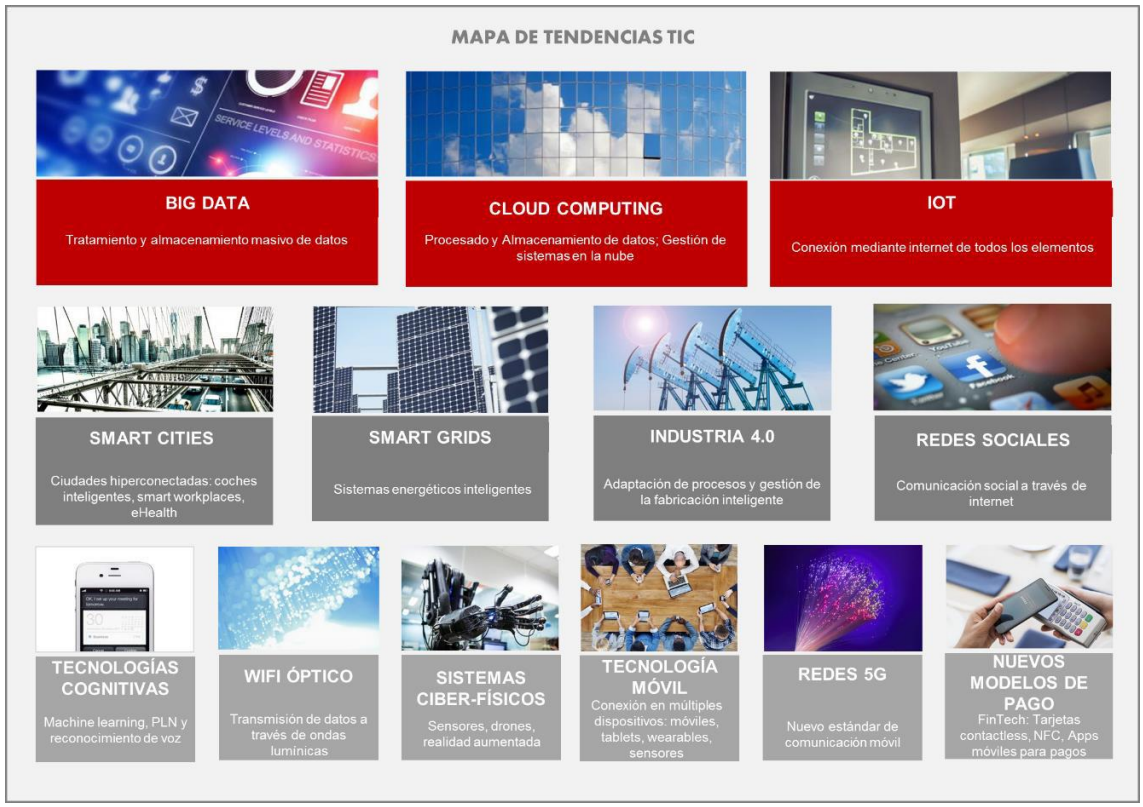
Núm.	Amenaces cloud computing	Riscos addicionals	Controls mitigants
9	***Due Diligence* insuficient**	- Les estratègies de negoci han de tenir en compte les tecnologies cloud en el seu procés d'avaluació per poder minimitzar el risc i implementar els controls adequats.	Els controls més destacats per aquest cas serien: - Assegurar que migrar al cloud segueix alineat amb els controls normatius / legals als quals està subjecte l'empresa. - Assegurar que els tècnics tenen coneixement de l'arquitectura cloud per poder adaptar l'arquitectura de seguretat. Controls mitigants a implementar segons CSA-CCM: *AIS-01, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BSR-09, BCR-10, BCR-11, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, IVS-06, IVS-09*
10 **(4,5,6)***	**Ús abusiu dels serveis cloud**	- Desplegaments de serveis cloud desenvolupats de forma insegura (trials gratuïts, comptes fraudulentes, ...) - DDoS attacks, spam, phishing, etc.	Els controls més destacats per aquest cas serien: - Detecció de pagaments fraudulents. - Plans de gestió d'incidents. - Definició de processos de denuncia d'abusos. Controls mitigants a implementar segons CSA-CCM: *HRS-01, HRS-02, HRS-03, HRS-04, HRS-07, HRS-08, HRS-10, SEF-01, SEF-02, SEF-03, SEF-04*
11 **(6)***	**Denegació de Servei (DoS)**	- El proveïdor de serveis cloud és un objectiu freqüent ja que engloba diversos serveis i permet realitzar atacs a més d'una organització a la vegada.	Els controls més destacats per aquest cas serien: - Aplicació de controls Anti-DDos. Controls mitigants a implementar segons CSA-CCM: *AIS-01, BCR-08, GRM-01, IVS-04*

Núm.	Amenaces cloud computing	Riscos addicionals	Controls mitigants
12	**Vulnerabilitats amb tecnologia compartida**	- La compartició d'elements d'infraestructura, arquitectura o aplicació, provoca que el compromís d'un sol component de tecnologia compartida exposi a tots els clients i podria arribar a afectar a tot el cloud.	Els controls més destacats per aquest cas serien: - Autenticació multi-factor a cada host. - Implementació de HIDS (Host-Based Intrusion Detection System). - Implementació de NIDS (Network Intrusion Detection System). - Segregació de xarxes. - Anti-malware i gestió de vulnerabilitats. Controls mitigants a implementar segons CSA-CCM: *DSI-04, EKM-03, GRM-01, IAM-02, IAM-05, IAM-12, IVS-01, IVS-09, TVM-02*

*** Correspondència amb les principals amenaces de la Taula 3.**

4.13.3. Mercat de serveis cloud

(INCIBE, 2016) En línia amb el Programa Europeu Horitzó 2020, el Cloud computing es troba dins les tres principals macro-tendències TIC.



Il·lustració 12. Mapa de les tendències TIC, horitzó 2020. (INCIBE, 2016)

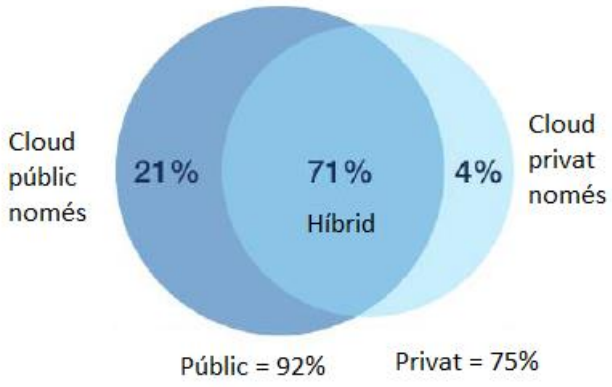
Aquest adquireix un protagonisme important convertint-se en un component essencial en les arquitectures de les aplicacions modernes, ja que permet un increment en les capacitats de les tecnologies, especialment les basades en tecnologies mòbils, analítiques i el processat de dades.

Els serveis de computació al núvol permeten la col·laboració massiva entorn de grans conjunts de dades, oferint solucions escalables i assequibles per la resolució de problemes computacionals.

Podríem dir que el cloud computing fomenta la disminució de la fractura digital entre grans i petites empreses.

(ISACA & CSA, Cloud Computing Market Maturity, 2015) Es tracta d'un mercat que està en creixement i constant evolució, i que encara no ha arribat al seu màxim nivell de maduresa. La seguretat i la privacitat continuen sent les principals preocupacions de les empreses a l'hora d'adoptar una tecnologia cloud, sobretot per la poca transparència dels proveïdors de serveis cloud, que no fan pública la informació de com garanteixen la seguretat per protegir els actius desplegats al cloud de possibles amenaces.

(Right Scale, 2018) Actualment, es podria dir que pràcticament totes les empreses utilitzen cloud a algun nivell, ja sigui públic o privat. L'estratègia preferida, de fet, és la implementació de multi-clouds. Els percentatges aproximats d'implementació de serveis cloud a les empreses queden reflectits a la següent il·lustració:



Il·lustració 13. Utilització del cloud per les organitzacions. (Right Scale, 2018)

Els principals proveïdors que ofereixen aquests serveis es mostren a la següent taula:

Taula 9. Principals proveïdors de cloud. (Berry, s.f.)

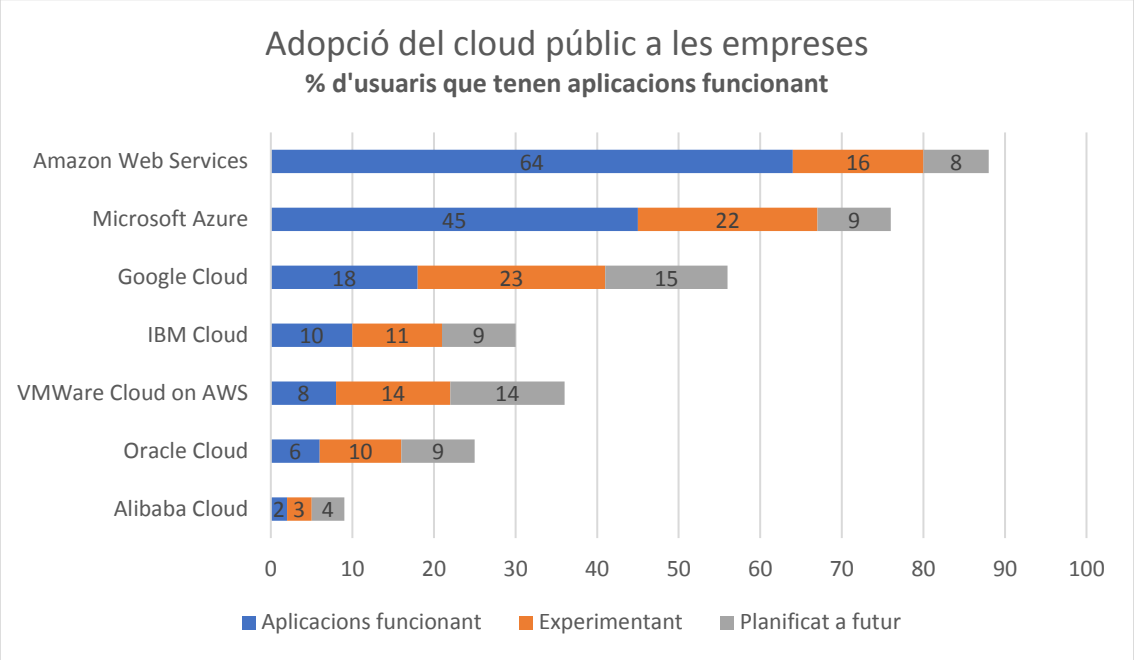
Proveïdor	IaaS	PaaS	SaaS	Emmagatzematge
Amazon	EC2 (Elastic Cloud Compute)	Amazon Web Services	Amazon Web Services	S3 (Simple Storage Service)
Google	n/a	Google App Engine (Python, Java, Go)	Google Aps	Google Cloud Storage
HP	Enterprise Services Cloud – Compute	Cloud Application Delivery	HP Software as a Service	Enterprise Services Cloud – Compute
IBM	SmartCloud Enterprise	SmartCloud Application Services	SaaS products	SmartCloud Enterprise – object storage
Microsoft	Microsoft Private Cloud	Windows Azure (includes .NET, Node.js, Java, PHP)	MS Office 365	Microsoft Private Cloud
JoyentCloud	SmartMachines	Node.js	n/a	n/a
Rackspace	Cloud Servers	Cloud Sites	Email & Apps	Cloud Files
Salesforce.com	n/a	Force.com	Salesforce.com	n/a
VMware*	VMware vSphere, vCloud	VMware vFabric (Java Spring), vCloud API	n/a	n/a

*VMware és un proveïdor de tecnologia subjacent al cloud computing i no ofereix serveis de host.

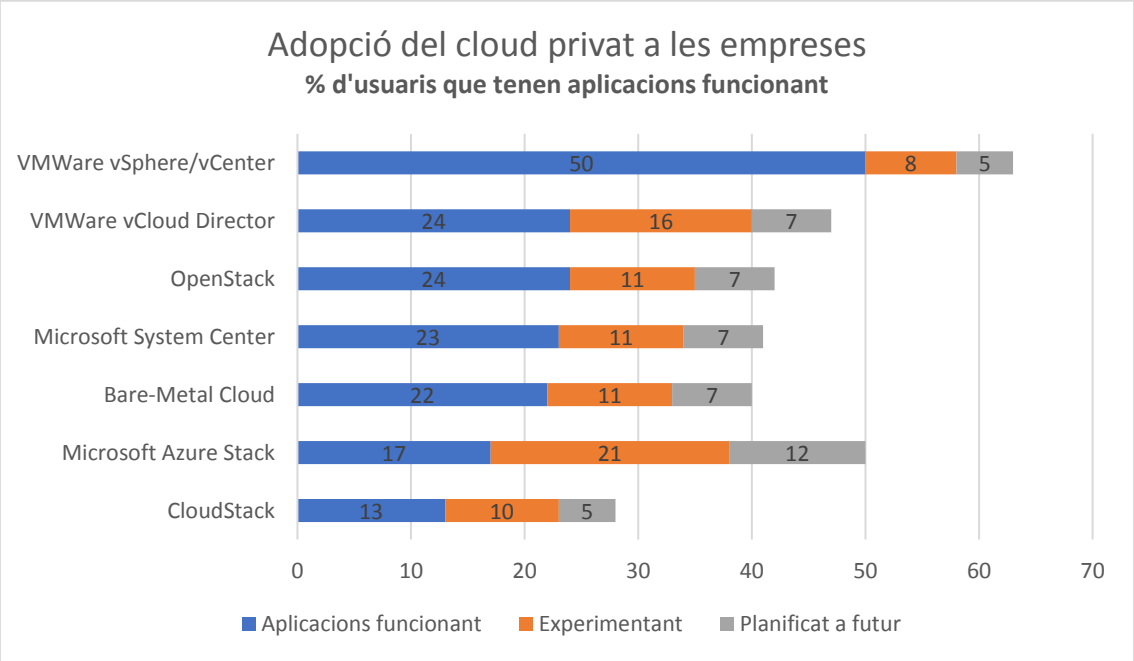
És important destacar que hi ha una gran diferència entre proveïdors segons els usuaris vulguin contractar un servei al cloud públic o cloud privat. A continuació, es mostren dues il·lustracions on es pot apreciar quins són els principals proveïdors per a cada tipus de model. Així com a nivell

de cloud públic, Amazon, Microsoft, Google i IBM s'emporten la major part del negoci, a nivell de cloud privat, VMware els hi guanya la partida, seguit de Microsoft.

A les il·lustracions es pot veure l'adopció dels serveis cloud a les empreses l'any 2018 dividit per aquelles que ja tenen aplicacions funcionant, les que estan experimentant i aquelles que pretenent utilitzar-ho a futur. Destacar que els percentatges que falten per arribar a 100 és aquelles empreses que no tenen aplicacions funcionant al cloud i que per tant no van contestar aquesta part de l'estudi.



Il·lustració 14. Adopció del cloud públic a les empreses. (Right Scale, 2018)



Il·lustració 15. Adopció del cloud privat a les empreses. (Right Scale, 2018)

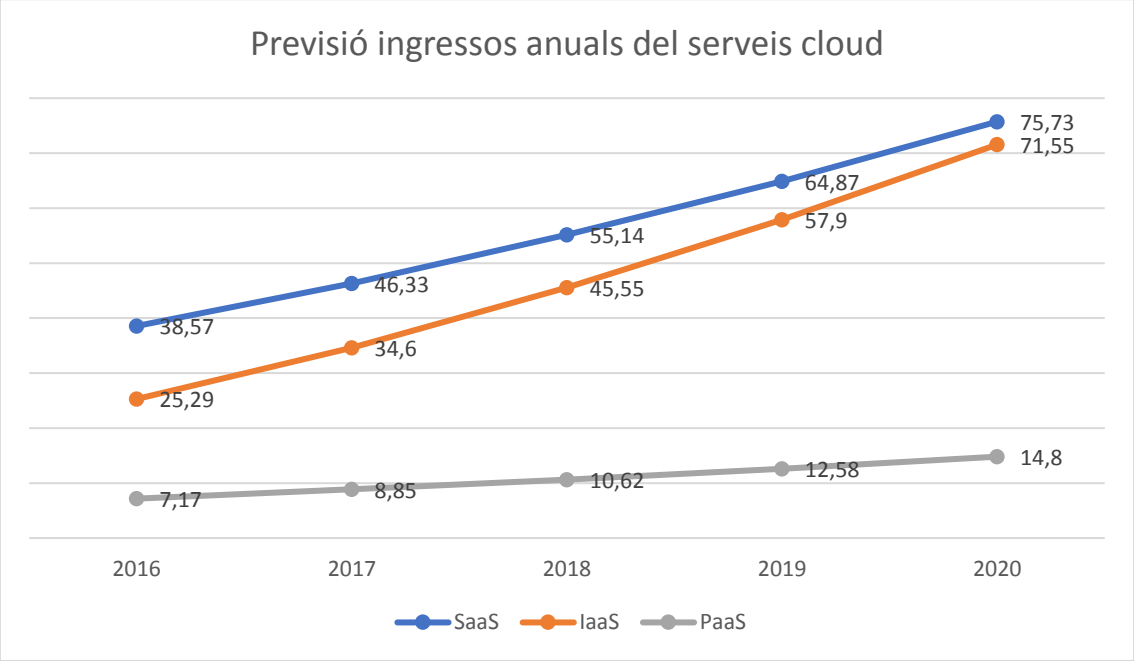
4.13.4. Rols i responsabilitats. Relació proveïdor de servei cloud amb usuari

Donat que el mercat cloud encara es troba en fase de maduració, presenta algunes mancances significatives. La més destacada és la repartició de rols i responsabilitats entre el proveïdor de serveis cloud i l'usuari. En aquest sentit, (ENISA, 2009) a diferència d'altres serveis, a l'hora de contractar un servei cloud cal prestar especial atenció a:

- les **garanties** que et dóna el proveïdor cloud a nivell de seguretat.
- les clàusules **legals** estàndard del contracte que fan referència als drets i obligacions en cas de fuga d'informació, transferència de dades, canvi de control i accés a les dades per part d'entitats de dret públiques. Addicionalment, també caldrà mirar les responsabilitats en cas d'interrupció de la infraestructura del cloud.

4.13.5. Inversió mundial a nivell cloud

(Gartner, 2018) Aquest any 2018, es preveu que la inversió mundial per serveis cloud sigui de més de 100 bilions de dòlars i es preveu que l'any 2020, la inversió mundial per serveis cloud serà aproximadament de 162 bilions de dòlars. És a dir, la inversió està previst que augmenti més d'un 30% en només 2 anys, fet que situa el cloud computing, efectivament, com un dels elements claus a tenir en compte per les empreses. A continuació, es mostra una gràfica que detalla també, quin és el model de servei més utilitzat:



Il·lustració 16. Previsió d'ingressos anuals dels serveis cloud. (Gartner, 2018)

4.13.6. Principals organismes

A part dels principals organismes ja mencionats en l'apartat 4.10, específicament per Cloud destaca la Cloud Security Alliance (CSA).

4.13.6.1. Cloud Security Alliance (CSA)

(CSA, 2018) És una organització sense ànim de lucre que té com a objectius:

- Promoure l'ús de bones pràctiques per garantir la seguretat de la informació dels serveis de Cloud Computing.
- Proporcionar informació sobre els possibles usos del Cloud Computing per ajudar a securitzar tots els altres sistemes informàtics inclosos al cloud.

Sorgí d'una iniciativa dins del ISSA CISO Forum a Las Vegas, l'any 2008 i el seu primer producte fou llençat a principis de l'any 2009.

No és un organisme regulador, sinó que està format fonamentalment per voluntaris que participen en diferents grups de recerca.

4.13.7. Directives / normatives associades al cloud

(ISACA & CSA, Cloud Computing Market Maturity, 2015) El mercat del cloud computing no té un criteri comú pel qual pugui mesurar la seguretat de la informació. Les següents organitzacions, CSA, ENISA, NIST i d'altres han publicat estudis i recomanacions de com mesurar-la però no hi ha un estàndard a seguir.

4.13.8. Marcs de control específics per serveis de cloud computing

La securització d'un entorn de cloud computing s'emmarca dins els controls definits prèviament en el punt 4.12 i no hi ha un conjunt de requeriments específics a complir per normativa. Tot i això, a continuació es mostren dos marcs de control que proposen requeriments específics pel cloud i que ens poden ajudar cara la seguretat del nostre entorn.

4.13.8.1. ISO/IEC 27017:2015

(ISO, 2015) La ISO/IEC 27017:2015 s'utilitza sempre conjuntament amb les normes ISO 27001 i ISO/IEC 27002, comentades en el punt 4.12.1, dóna unes directrius de seguretat de la informació aplicables a l'aprovisionament i l'ús de serveis cloud mitjançant:

- Directrius addicionals per aquells controls considerats rellevants i especificats en la ISO/IEC 27002.
- Controls addicionals específics per serveis cloud.

Destacar que els controls es donen tant a nivell del proveïdor de serveis cloud com del consumidor d'aquests serveis.

4.13.8.2. CSA-CCM (Cloud Security Alliance – Cloud Controls Matrix)

(CSA, 2017) La CSA-CCM està dissenyada específicament per proporcionar principis de seguretat fonamentals per guiar als venedors i potencials usuaris finals amb l'avaluació del risc general de seguretat d'un proveïdor al núvol. La implementació d'aquesta matriu de controls serveix a les organitzacions per:

- Reforçar els controls de seguretat de la informació existents reduint les amenaces de seguretat i vulnerabilitats pròpies del núvol.
- Proporcionar una seguretat estandarditzada i una gestió dels riscos operatius.
- Normalitzar les expectatives de seguretat, la taxonomia del núvol i la terminologia i mesures de seguretat implementades al núvol.

Addicionalment, destacar que es complementa amb altres estàndards de seguretat i normatives reconegudes en el món de la ciberseguretat com podrien ser la ISO 27001/27002, COBIT, PCI, NIST.

En concret, la CSA-CCM consta de 133 objectius de control alineats amb els 13 principals dominis de seguretat definits per la CSA.

Taula 10. Principals dominis de seguretat definits per la CSA.

	Domini	Núm. de controls
	Seguretat d'aplicació i d'interfície	4
	Garantia d'auditoria i compliment normatiu	3
	Continuïtat del negoci i resiliència operativa	11
	Control de canvis i gestió de la configuració	5
	Seguretat de les dades i gestió del cicle de vida de la informació	7
	Seguretat del CPD (centre de processament de dades)	9
	Encriptació i gestió de claus	4
	Govern i gestió del risc	11
	Recursos humans	11
	Gestió d'accessos i identitats	13
	Seguretat de la infraestructura i la virtualització	13
	Interoperabilitat i portabilitat de les APIs	5
	Seguretat mòbil	20
	Gestió d'incidents de seguretat, E-discovery i cloud forense	5
	Gestió de la cadena de subministrament, transparència i rendició de comptes (responsabilitat)	9
	Gestió d'amenaces i vulnerabilitats	3

5. Metodologia

5.1. Anàlisi de riscos com a element clau per garantir la seguretat de la informació

Durant els objectius del treball, s'ha plantejat la idea que per garantir la seguretat de la informació d'una empresa, l'element clau és la identificació els riscos existents i la implementació dels controls compensatoris per a mitigar-los. Per això es proposa la realització d'un anàlisi de riscos d'una organització juntament amb la implementació de tots els controls que se'n deriven.

Cal destacar l'alta sensibilitat de les dades tractades i que aquestes dades són subjectes de ser guardades en ubicacions específiques però també transmeses via diferents canals per finalitats de negoci.

Per justificar aquest plantejament, a continuació es mostren diverses fonts oficials que aposten per la gestió del risc com el punt principal per garantir la seguretat de la informació d'una organització. Totes elles ens poden ajudar a la identificació del risc en base a uns estàndards de classificació i marcs de control disponibles.

ISO 31000:2009 Risk Management – Principles and Guidelines

(ISO, 2009) Aquest estàndard internacional recomana que les organitzacions desenvolupin, implementin i millorin contínuament un marc de controls amb la finalitat d'integrar el procés de gestió del risc dins del govern, planificació, estratègia, gestió, polítiques, valors i cultura d'una organització.

L'enfoc genèric de la gestió del risc descrit en aquest estàndard proporciona els principies i les directrius per gestionar qualsevol tipus de risc d'una forma sistemàtica, transparent i creïble dins d'un abast i un context determinat.

ISO 31000:2009 Risk Management – Risk Assessment Techniques

(ISO, 2009) Afirma que totes les organitzacions s'enfronten a un conjunt de riscos que poden afectar a la consecució dels seus objectius.

Totes les activitats d'una organització tenen un risc que s'ha de gestionar. El procés de gestió del risc ajuda a l'equip directiu en la presa de decisions tenint en compte la possibilitat d'esdeveniments futurs o circumstàncies que puguin tenir efectes negatius envers als objectius definits.

ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements

(ISO, 2013) Afirma que l'organització ha de definir i aplicar un anàlisi de riscos de seguretat de la informació que identifiqui:

- Riscos associats amb la pèrdua de la confidencialitat, integritat i disponibilitat de la informació dins de l'abast de la gestió de la seguretat de la informació.
- Responsables d'aquests riscos.

NIST Special Publications

El NIST té moltes publicacions especials disponibles a csrc.nist.gov. Algunes d'elles estan relacionades amb el risc IT:

NIST Special Publications 800-30 Revision 1: Guide for conducting Risk Assessments

(NIST, 2012) Afirma que els anàlisis de riscos són clau en l'efectivitat de la gestió del risc i faciliten la presa de decisions tant a nivell organitzatiu, com de negoci com del propi sistema d'informació.

Donat que el procés de gestió de riscos és continuat, els anàlisis de riscos es realitzen mitjançant un procés SDLC (System Development Life Cycle o el cicle de vida del desenvolupament del sistema). És a dir, abans de l'adquisició del sistema, durant la implementació del sistema i finalment al llarg del manteniment del mateix.

NIST Special Publications 800-39: Managing Information Security Risks

(NIST, 2011) Proporciona un enfocament estructurat però flexible per la gestió del risc de forma generalitzada però emfatitzant sobretot en l'anàlisi, resposta i monitorització del risc de forma continuada mitjançant les pautes i estàndards de seguretat definits en el propi NIST.

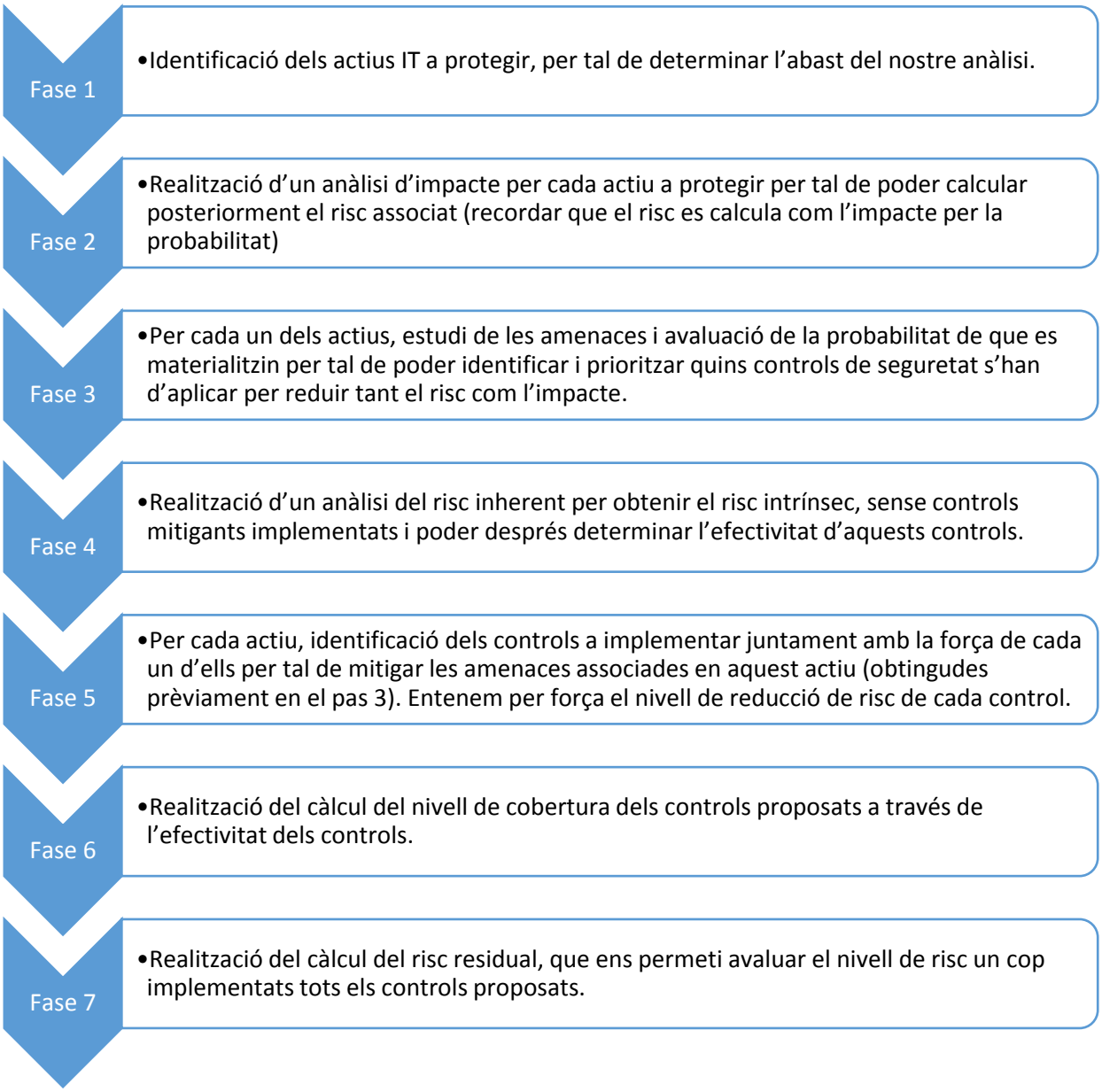
COBIT 5 for Risk

(ISACA, 2013) Proporciona un marc de controls comprensible que ajuda a les empreses a aconseguir els seus objectius de govern i gestió de la tecnologia de la informació. Ajuda a crear un valor òptim de la part IT a base de mantenir un equilibri entre els beneficis i la optimització tant dels nivells de risc com de la utilització dels actius.

5.2. Metodologia per la realització d'un anàlisi de riscos

En el nostre cas es realitzarà un anàlisi basat en una combinació del compliment de certs estàndards i en el risc (veure més detall al punt 3.1.4) i utilitzant el mètode ascendent (veure més detall al punt 3.1.2). L'objectiu és trobar el nivell de risc / exposició a amenaces de ciberseguretat per cada un dels actius a protegir.

Basant-nos en la metodologia descrita per (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012) i (INCIBE, 2017) es proposen les següents fases:


Fase 1
•Identificació dels actius IT a protegir, per tal de determinar l'abast del nostre anàlisi.
Fase 2
•Realització d'un anàlisi d'impacte per cada actiu a protegir per tal de poder calcular posteriorment el risc associat (recordar que el risc es calcula com l'impacte per la probabilitat)
Fase 3
•Per cada un dels actius, estudi de les amenaces i avaluació de la probabilitat de que es materialitzin per tal de poder identificar i prioritzar quins controls de seguretat s'han d'aplicar per reduir tant el risc com l'impacte.
Fase 4
•Realització d'un anàlisi del risc inherent per obtenir el risc intrínsec, sense controls mitigants implementats i poder després determinar l'efectivitat d'aquests controls.
Fase 5
•Per cada actiu, identificació dels controls a implementar juntament amb la força de cada un d'ells per tal de mitigar les amenaces associades en aquest actiu (obtingudes prèviament en el pas 3). Entenem per força el nivell de reducció de risc de cada control.
Fase 6
•Realització del càlcul del nivell de cobertura dels controls proposats a través de l'efectivitat dels controls.
Fase 7
•Realització del càlcul del risc residual, que ens permeti avaluar el nivell de risc un cop implementats tots els controls proposats.

6. Cas pràctic

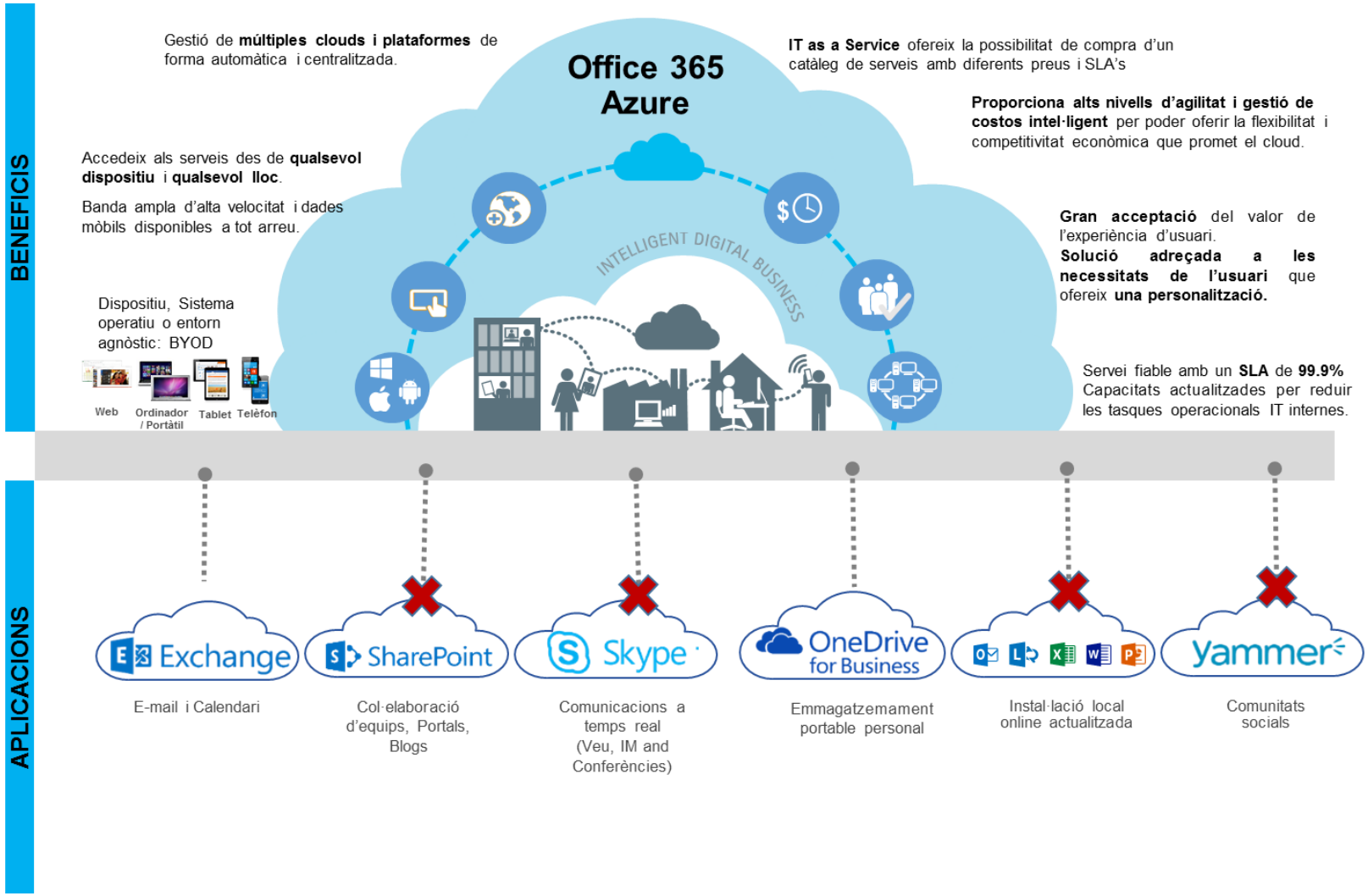
Segons la metodologia proposada en el punt 5, es procedirà a realitzar l'anàlisi de riscos associat a una solució basada en cloud per la implementació de l'Office365 (Exchange i One-drive) a Azure . Destacar que pel cas pràctic es realitzarà un **anàlisis de riscos de la solució** i no un anàlisis de riscos a nivell de tota l'entitat.

S'ha triat la migració cap a l'Office365 per la seva aplicabilitat a moltes empreses actuals que busquen oferir als seus treballadors accés al contingut des de qualsevol dispositiu (corporatiu o personal, portàtil, tablet, mòbil...), en qualsevol moment i des de qualsevol lloc del món. És una solució que permet a les empreses estar al dia en la seva agenda digital i actualitzades en les noves tendències del mercat.

Com s'ha comentat a la Il·lustració 14, les solucions de Microsoft Azure són les que estan més esteses a les empreses darrera dels Amazon Web Services, per tant, s'ha considerat pertinent realitzar aquest anàlisi.

6.1. Migració al cloud mitjançant Office365

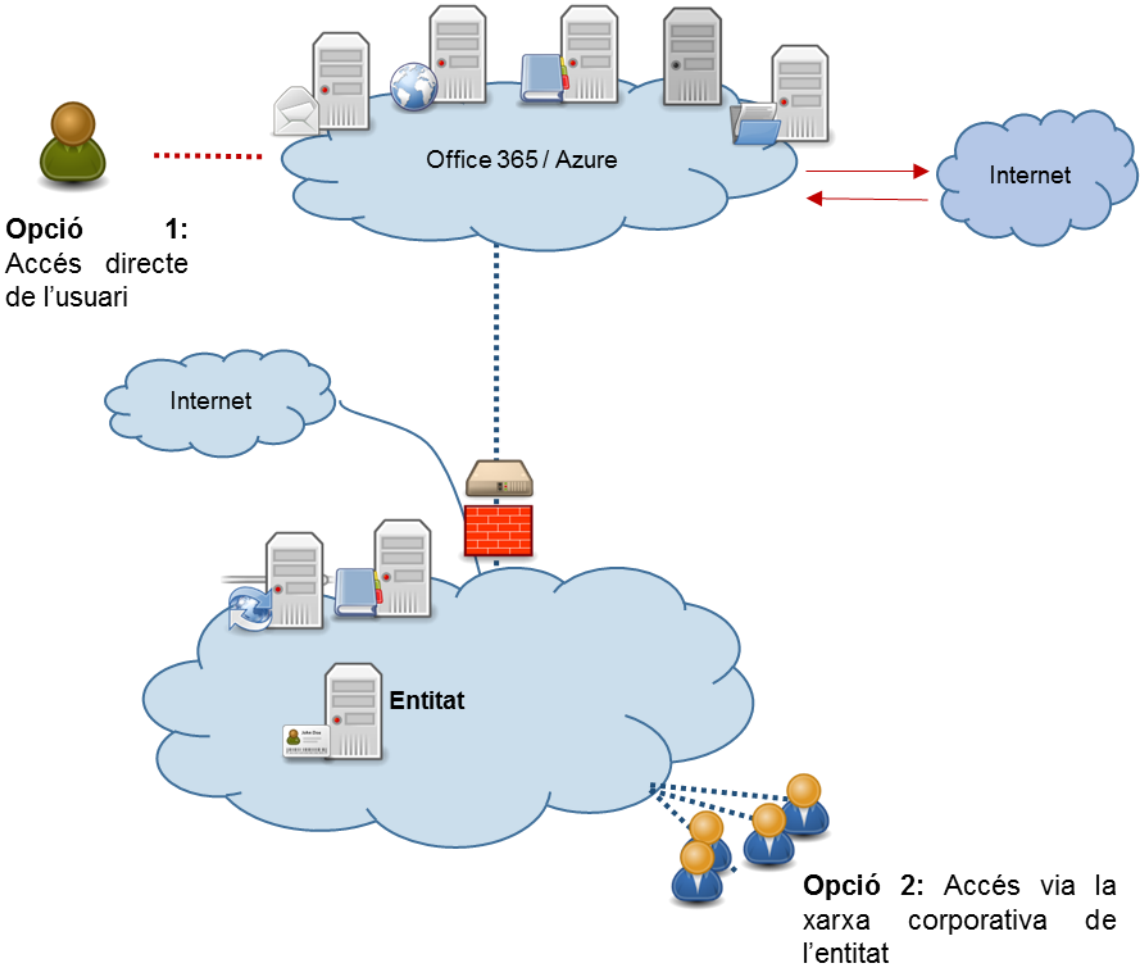
A continuació es mostra una il·lustració de la solució completa d'Office 365 i es marcarà amb una creu aquelles aplicacions que quedaran fora de l'abast d'aquest anàlisi de riscos. La selecció s'ha fet en funció de la criticitat i s'ha suposat que per la resta d'aplicacions, amb els controls proposats per l'exchange i el one-drive també es garantiria la seguretat.



Il·lustració 17. Solució Office365 al cloud.

6.1.1. Diagrama de l'entorn a migrar al cloud

El que es vol securitzar és tant l'accés de l'usuari directament a Office 365 (opció 1), com l'accés de l'usuari via la xarxa corporativa de l'entitat (opció 2). A sota s'adjunta una il·lustració de la solució sobre la qual es farà l'anàlisi de riscos.



Il·lustració 18. Proposta de solució a analitzar.

6.1.2. Requeriments de seguretat

Els requeriments a tenir en compte per garantir la seguretat de l'entorn de correu són dades reals provinents d'una sol·licitud realitzada per una entitat que es mantindrà en l'anonimat i són els següents:

Taula 11. Requeriments de seguretat a tenir en compte per la solució Office365 al cloud.

Domini	ID	Requeriment
Correu entrant	Req 1	Antivirus i Antispam al perímetre. Tots els correus entrants han de passar per un filtre d'AV i Anti-Spam abans d'arribar al servidor de correu. Allà el correu serà redirigit a la xarxa interna de l'entitat o al servei cloud depenent de l'objectiu.
	Req 2	Antivirus i Antispam als servidors de correu. Els servidors de correu han de tenir sistemes d'anti-virus i anti-spam per permetre que el contingut de la bústia sigui escanejat. Idealment, les tecnologies implementades haurien de ser diferents a les utilitzades per protegir el perímetre.
	Req 3	Capacitat TLS per les connexions amb tercers.
Correu sortint / fuga d'informació	Req 4	Restringir el contingut del correu enviat en base a la mida i el tipus d'adjunt. Contingut actiu a l'adjunt ha d'estar controlat.
	Req 5	Anti-virus i anti-spam pel correu sortint
	Req 6	Desplegament DLP integrat amb el DLP corporatiu. Aquest ha de permetre la detecció de certes expressions regulars i de contingut indexat en recursos interns.
Control d'accés i autenticació	Req 7	Requerir l'autenticació segura de l'usuari i la integració amb AD
	Req 8	Restringir l'accés a les bústies de correu pròpies i autoritzades i tenir un procediment d'accés a altres bústies de correu
	Req 9	Limitar els protocols d'accés al correu des de dispositius mòbils o altres dispositius finals, que haurien d'estar securitzats mitjançant una solució MDM
	Req 10	Protegir l'accés web al correu mitjançant encriptació (TLS) i autenticació i restringir l'accés via web al correu electrònic només des de xarxa interna o via la extranet (VPN SSL).
	Req 11	Monitorització i detecció d'accessos no autoritzats, activitats malicioses o violacions de la política de seguretat de l'entitat.
Monitorització	Req 12	Assegurar la recol·lecta de logs a diferents capes de la infraestructura a temps real (cada 10 minuts). Incloent els logs dels usuaris administradors.
	Req 13	Els logs generats per Microsoft han de tenir el mateix format o s'han de poder integrar amb el SIEM corporatiu de l'entitat.
	Req 14	Permetre el servei Journaling amb la mateixa configuració que l'entitat i un període de retenció de 5 anys dins els servidors Exchange d'Office 365 per assegurar que es poden realitzar anàlisis forenses.
	Req 15	Tractament dels logs alineats a la política de l'entitat. L'accés ha d'estar restringit, protegit i revisat de forma periòdica.
Backup e-mail	Req 16	Aplicar la mateixa política de backup que l'entitat que contempla una retenció de 10 anys, encara que s'acabi la prestació del servei.
	Req 17	Restaurar les bústies de correu a temps real.
	Req 18	El Reporting del rendiment dels backups ha d'estar sempre disponible.
	Req 19	Replicacions de l'Exchange Online per garantir la continuïtat del servei.
Encriptació / protecció e-mail	Req 20	Permetre l'encriptació i la signatura electrònica dels correus interns

Domini	ID	Requeriment
	Req 21	Permetre l'encriptació i la signatura electrònica dels correus enviats a direccions externes. Integració amb solucions gateway externes encriptades i firmades o enviament d'enllaços al missatge protegit
	Req 22	Permetre reconèixer correus externs signats electrònicament
	Req 23	Permetre la gestió de contingut protegit amb DRM tant pels correus entrants com sortints.
Seguretat Comunicacions	Req 24	Encriptació (TLS) de la comunicació entre el dispositiu de l'usuari i el servidor exchange
	Req 25	Restringir les connexions a adreces IP de l'entitat
Compliance	Req 26	Assegurar l'accés i la possibilitat de realitzar cerques a totes les bústies de correu.
Migració de dades	Req 27	Permetre exportar dades
Correus electrònics proveïdors	Req 28	Autenticació DMARC. Es pot trobar el detall en el punt 3.2.5.3.6.
	Req 29	Configurar regles pre-definides

6.1.3. Identificació de les mesures de seguretat natives d'Office365

Per tal de poder fer l'anàlisi de riscos, s'ha fet una recerca sobre les mesures de seguretat que ja té implementades de forma intrínseca Office365.

Revisant el document de (Microsoft corporation, 2015), on s'inclou una explicació de com Office365 compleix amb els controls de seguretat detallats a la CSA-CM i amb la documentació proporcionada per Microsoft respecte la seguretat inclosa en la solució d'Office365 (Microsoft Corporation, 2018), s'han identificat les següents mesures de seguretat pròpies d'Office 365 (Nota: apliquen les mateixes per One-drive i per Exchange). A continuació es mostra un resum, el detall de les solucions es pot trobar al punt 3.2.5.3.

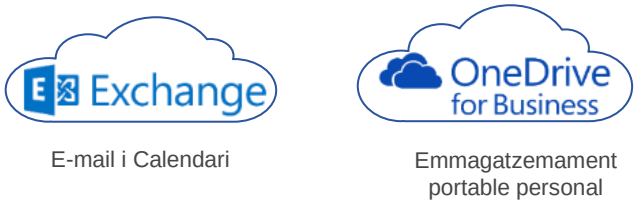
Taula 12. Mesures de seguretat pròpies d'Office365.

Mesures de seguretat	Exchange i One-drive
AV entrant	• Els missatges entrants s'escanegen per la detecció de malware (virus i spam). • En cas de detectar malware, el missatge és esborrat o reemplaçat amb un adjunt que indica amb un missatge per defecte de la detecció de malware. **Nota**: es poden enviar notificacions als emissors o administradors quan un missatge és esborrat
Anti-SPAM (entrant i sortint)	• Aquest servei proporciona filtres de connexió i filtratge de contingut per tots els missatges entrants. El filtre de correu brossa de sortida també està sempre activat.
Autenticació i autorització	• Permet el control d'accés i la gestió de comptes privilegiades
Múltiple factor d'autorització	• El múltiple factor d'autenticació ajuda a securitzar el procés de login d'usuari més enllà de només una simple contrasenya.
DLP	• Permet establir polítiques per protegir dades sensibles • Detecta la informació sensible mitjançant la classificació de missatges i la indexació de documents
RMS	• Permet protegir arxius i correus electrònics importants com ara Excels, Words, etc.
BYOK	• Permet a les organitzacions xifrar les seves dades i mantenir el control de la gestió de les seves claus de xifrat.
Lockbox	• Permet controlar com es vol que els enginyers de Microsoft accedeixin a les dades de l'entitat en cas de necessitar ajuda per la resolució d'un incident o configuració del cloud.

Un cop identificades les mesures ja es pot procedir amb l'anàlisi de riscos de la solució seguint els passos descrits en el punt 5.

6.2. Fase 1: Identificació d'actius

Tal i com es pot veure en la Il·lustració 17, els actius que entren dins l'abast de l'anàlisi de riscos proposat són l'exchange (correu electrònic i calendari) i l'emmagatzemament portable personal (One Drive):



E-mail i Calendari

Emmagatzemament portable personal

Il·lustració 19. Actius identificats per l'anàlisi de riscos.

6.3. Fase 2: Resultats anàlisi d'impacte de la solució

Es començarà fent una anàlisi d'impacte. Destacar que aquest és comú per les dues opcions d'accés ja que no té en compte els controls implementats.

6.3.1. Mètode càlcul d'impacte

Per cada actiu identificat prèviament, es realitzarà un anàlisi de l'impacte a nivell de confidencialitat, integritat i disponibilitat que suposaria el compromís del mateix. L'objectiu és obtenir un valor del nivell de l'impacte que suposaria un ciberatac a cada un dels actius identificats.

Primer haurem d'identificar els principals impactes derivats d'un ciberatac.

(CCN-CERT, 2017) Segons l'informe de ciberamenaces i tendències publicat pel CCN- CERT, els costos més significatius per les empreses derivats d'un ciberatac són: costos econòmics, costos de temps d'inactivitat, pèrdua de dades sensibles (ja sigui per fuga o per robatori) i pèrdua de vides (en el cas que l'incident passi en un hospital o alguna altra institució mèdica). En el nostre cas, descartarem l'últim cost ja que estem analitzant una entitat financera i no una entitat mèdica.

En conseqüència, l'impacte s'avaluarà a nivell:

- **Econòmic**: suposa, valgui la redundància, pèrdues econòmiques a l'empresa.
- **Operacional**: suposa una aturada dels sistemes / processos de l'empresa.
- **Legal**: inclou infraccions contractuals, accions reguladores per incompliments normatius, implicacions legals (incloent multes i càrrecs penals a persones).
- **Reputació:** suposa la pèrdua de la confiança o bona opinió de la societat envers l'organització.

En segon lloc identificarem el pes dels principals impactes identificats

Donat que no tots els impactes tenen les mateixes conseqüències per les organitzacions, ja que un impacte econòmic o legal suposa unes pèrdues molt més elevades que un impacte operacional o de reputació, s'assignarà pesos diferents a l'hora de realitzar el càlcul de l'impacte total. Així doncs assignarem:

- 1/3 impacte econòmic.
- 1/3 impacte legal.
- 1/6 impacte de reputació.
- 1/6 impacte operacional.

En tercer lloc, identificarem l'escala pel càlcul de l'impacte:

Per tal de definir l'escala primer s'han de marcar els diferents valors que pot prendre l'impacte. En aquest cas s'ha considerat:

- Molt baix.
- Baix.
- Mitjà.
- Alt.
- Molt alt.

Un cop es tenen els valors, s'ha de procedir a analitzar els **límits establerts** per canviar de nivell. En aquest sentit destaquem que:

- A nivell econòmic s'ha tingut en compte la dada comentada al punt 4.6, que especificava que el cost resultat d'una filtració d'informació l'any 2017 per grans empreses, de mitjana, és d'$1.3 milions. Així doncs, considerarem com a un impacte alt tot el que

estigui per sobre d'1 milió d'euros. A partir d'aquí, la resta s'han adaptat perquè tinguin un sentit més o menys lineal.

- A nivell operacional s'ha realitzat una recerca sobre els RTO (Recovery Time Objective) que es demanen als bancs. (Marlin, 2017) Segons una proposta realitzada pel FDIC (Federal Deposit Insurance Corporation) i l'Office of the Comptroller of the Currency (dos entitats reguladores dels estats units), els bancs s'haurien de recuperar d'un ciberatac en menys de dues hores. Per aquesta raó, s'ha agafat com a límit les dues hores per considerar que l'impacte operacional és baix. (IBM, 2018) La resta d'impactes estan posats sobre els valors més utilitzats per definir l'RTO.

A continuació es mostra la taula amb l'escala finalment decidida:

Taula 13. Escala de valoració d'impacte.

Valor	Impacte	Reputació	Econòmic	Legal	Operacional
1	(1) Molt baix	Cap impacte a nivell de clients i/o mercat	Cap implicació econòmica	Cap implicació o incompliment legal o normatiu.	Cap impacte a nivell operatiu.
2	(2) Baix	Inconveniències menors per tots els clients	Els costos econòmics directes o indirectes són per sota els 500.000€	Fora de termini/ infracció contractual menor.	Interrupcions lleus de les operacions (p.e. rendiment baix i/o un temps de recuperació <2 hores)
3	(3) Mitjà	Inconveniències menors afectant la majoria de clients i inconveniències greus afectant pocs clients.	Els costos econòmics directes o indirectes estan entre els 500.000€ i el milió d'euros.	Accions reguladores (sense multa) i/o accions legals per infraccions contractuals significatives.	Interrupcions significatives en les operacions (p.e. indisponiblitat a curt termini i/o un temps de recuperació <4 hores)
4	(4) Alt	Inconveniències greus afectant tots els clients i amb una repercussió als mitjans de comunicació i a nivell normatiu.	Els costos econòmics directes o indirectes estan per sobre del 1.000.000€	- Multes greus per incompliment normatiu - Accions reguladores per incompliments normatius - Implicacions legals greus (incloent multes i càrrecs penals a persones).	Greus interrupcions en les operacions (p.e. indisponiblitat a mig termini i/o temps de recuperació d'1 dia).
5	(5) Molt alt	Els serveis no estan disponibles durant diversos dies amb una repercussió als mitjans de comunicació i a nivell normatiu.	Els costos econòmics directes o indirectes estan per sobre dels 5.000.000€	- Multes molt greus per incompliment normatiu - Accions reguladores per incompliments normatius - Implicacions legals molt greus (incloent multes i càrrecs penals a persones).	Canal de distribució deshabilitat / Interrupció total de les operacions / Temps de recuperació de més d'1 dia

En quart lloc, es procedirà a realitzar l'anàlisi de l'impacte segons la confidencialitat, integritat i disponibilitat dels diferents dominis:

Confidencialitat

Taula 14. Anàlisi d'impacte segons la confidencialitat.

Actiu	Impacte Confidencialitat (IC)	Impacte econòmic (IE)	Impacte de Reputació (IR)	Impacte Legal (IL)	Impacte operacional (IO)	Justificació
Actiu identificat en el punt 6.2	Calculat com: $IC = \frac{1}{3}IE + \frac{1}{3}IL + \frac{1}{6}IR + \frac{1}{6}IO$	Valor de l'1 al 5 considerat segons l'escala definida.	Valor de l'1 al 5 considerat segons l'escala definida.	Valor de l'1 al 5 considerat segons l'escala definida.	Valor de l'1 al 5 considerat segons l'escala definida.	Suposicions i justificacions dels valors d'impacte triats.

Integritat

Taula 15. Anàlisi d'impacte segons la integritat.

Actiu	Impacte Integritat (II)	Impacte econòmic (IE)	Impacte de Reputació (IR)	Impacte Legal (IL)	Impacte operacional (IO)	Justificació
Actiu identificat en el punt 6.2	Calculat com: $II = \frac{1}{3}IE + \frac{1}{3}IL + \frac{1}{6}IR + \frac{1}{6}IO$	Valor de l'1 al 5 considerat segons l'escala definida.	Valor de l'1 al 5 considerat segons l'escala definida.	Valor de l'1 al 5 considerat segons l'escala definida.	Valor de l'1 al 5 considerat segons l'escala definida.	Suposicions i justificacions dels valors d'impacte triats.

Disponibilitat

Taula 16. Anàlisi d'impacte segons la disponibilitat.

Actiu	Impacte Disponibilitat (ID)	Impacte econòmic (IE)	Impacte de Reputació (IR)	Impacte Legal (IL)	Impacte operacional (IO)	Justificació
Actiu identificat en el punt 6.2	Calculat com: $ID = \frac{1}{3}IE + \frac{1}{3}IL + \frac{1}{6}IR + \frac{1}{6}IO$	Valor de l'1 al 5 considerat segons l'escala definida.	Valor de l'1 al 5 considerat segons l'escala definida.	Valor de l'1 al 5 considerat segons l'escala definida.	Valor de l'1 al 5 considerat segons l'escala definida.	Suposicions i justificacions dels valors d'impacte triats.

Finalment es presentarà un resum de l'anàlisi d'impacte en el següent format:

Taula 17. Resum anàlisi d'impacte.

Actiu	Confidencialitat	Integritat	Disponibilitat
Actiu identificat en el punt 6.2	Valor Impacte Confidencialitat de la Taula 14.	Valor Impacte Integritat de la Taula 15.	Valor Impacte Disponibilitat de la Taula 16.

6.3.2. Resultats càlcul impacte

A continuació es mostren els resultats obtinguts pel càlcul de l'impacte dels diferents actius:

Taula 18. Resultat anàlisi d'impacte segons la confidencialitat.

CONFIDENCIALITAT						
Actius	**Impacte Confidencialitat (IC)**	**Impacte econòmic (IE)**	**Impacte de Reputació (IR)**	**Impacte Legal (IL)**	**Impacte operacional (IO)**	**Justificació**
Exchange	**3,8**	4	4	5	3	Assumint que es podrien produir fugues d'informació de dades de nivell alt, al comprometre la confidencialitat es podrien donar accessos a informació sensible de la organització per part d'usuaris no autoritzats o d'atacants externs. Tot i que les dades més crítiques no haurien de ser enviades a través d'aquest canal, l'exposició d'alguna informació del correu electrònic podria suposar impacte legal i de reputació.
One-drive	**3,8**	4	4	5	3	Al comprometre la confidencialitat es podrien donar accessos a informació sensible de la organització per part d'usuaris no autoritzats o d'atacants externs.

Taula 19. Resultat anàlisi d'impacte segons la integritat.

INTEGRITAT						
Actius	**Impacte Integritat (II)**	**Impacte econòmic (IE)**	**Impacte de Reputació (IR)**	**Impacte Legal (IL)**	**Impacte operacional (IO)**	**Justificació**
Exchange	**3,0**	3	3	3	3	Davant la pèrdua o la modificació no autoritzada de les dades, la operativa de la organització es veuria altament afectada, al tractar-se d'una eina crítica de comunicació que també pot contenir informació d'alta importància de cara a complir els objectius de negoci.
One-drive	**3,0**	3	3	3	3	Davant la pèrdua o la modificació no autoritzada de les dades, la operativa de la organització es veuria altament afectada, al tractar-se d'una eina crítica de comunicació que també pot contenir informació d'alta importància de cara a complir els objectius de negoci.

Taula 20. Resultat anàlisi d'impacte segons la disponibilitat.

DISPONIBILITAT						
Actius	**Impacte Disponibilitat (ID)**	**Impacte econòmic (IE)**	**Impacte de Reputació (IR)**	**Impacte Legal (IL)**	**Impacte operacional (IO)**	**Justificació**
Exchange	**4,3**	4	4	4	5	La indisponiblitat del correu corporatiu d'una organització pot suposar un greu impacte en la seva operativa diària, afectant tant al seu funcionament intern com a la part de negoci. La manca de comunicació a través d'aquest canal també podria provocar incompliments de regulació, afectació en objectius de negoci o danys de reputació davant de proveïdors i clients.
One-drive	**4,3**	4	4	4	5	La indisponiblitat de l'emmagatzemament d'una organització pot suposar un greu impacte en la seva operativa diària, afectant tant al seu funcionament intern com a la part de negoci.

A continuació s'inclou una taula resum en la que es pot veure que, l'impacte a nivell de confidencialitat, integritat i disponibilitat dels diferents actius és mig:

Taula 21. Taula resum de l'impacte per cada actiu.

RESUM			
Actius	**Impacte Confidencialitat**	**Impacte d'Integritat**	**Impacte de Disponibilitat**
Exchange	**3,8**	**3,0**	**4,3**
One-drive	**3,8**	**3,0**	**4,3**

6.4. Fase 3: Amenaces i avaluació de la probabilitat

Abans de poder avaluar els riscos de seguretat que afronta una organització, cal definir un catàleg de totes aquelles amenaces que li apliquen. En aquest sentit, l'objectiu és obtenir un catàleg de les diferents amenaces que apliquen i avaluar la probabilitat d'ocurrència d'aquestes.

Definirem el catàleg basant-nos amb les principals amenaces actuals de seguretat específiques per un entorn cloud, comentades en el punt 4.13.2.

A continuació s'inclou l'escala a tenir en compte per la definició de la probabilitat:

Taula 22. Nivells de risc.

Nivell de risc	Valor del risc (probabilitat x impacte)
Molt baix	Pràcticament impossible que es materialitzi
Baix	Es pot materialitzar en els propers 10 anys
Mitjà	Es pot materialitzar en els propers 2-3 anys
Alt	Es pot materialitzar abans d'un any
Molt Alt	Es pot materialitzar en els propers mesos

Taula 23. Amenaces i probabilitat d'ocurrència.

ID Amenaça	Amenaça	Riscos Addicionals	Probabilitat	Probabilitat	Justificació
AM_1	**Fuga d'informació**	- Recursos de xarxa compartits. - Personal del proveïdor cloud i els seus dispositius. - Tercers contractats pel proveïdor de cloud. - Quantitat de dades disponibles al cloud de forma centralitzada. Destacar que els proveïdors de cloud tenen seguretat desplegada per tot allò que consideren que és responsabilitat seva, però són els clients qui són responsables de protegir les seves dades dins del cloud.	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.
AM_2	**Pobre gestió d'identitats, credencials i accessos**	- Federació d'identitats amb el proveïdor cloud (p.e. SAML). - Centralització dels sistemes d'emmagatzemat de dades crítiques (contrasenyes, claus privades, ...).	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.
AM_3	**APIs no segures**	- Exposició de interfícies d'usuaris (UI) o interfícies de programa d'aplicació (APIs) que els clients utilitzen per interactuar amb els serveis cloud i realitzar l'aprovisionament, la gestió, les operacions i la monitorització dels seus sistemes. - Compartició de credencials amb tercers per part dels usuaris de cloud, degut a l'existència d'una doble capa d'APIs, ja que les organitzacions construeixen els seus serveis sobre les APIs existents dels proveïdors cloud.	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.

ID Amenaça	Amenaça	Riscos Addicionals	Probabilitat	Probabilitat	Justificació
AM_4	**Vulnerabilitats de sistema i aplicació**	- Amb l'aparició dels multi-tenants i el cloud computing, els sistemes de diverses organitzacions es troben "a prop", compartint memòria, recursos, infraestructura, etc.	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.
AM_5	**Apropiació indeguda de comptes**	- Si un atacant té accés a les credencials d'un client de cloud, pot utilitzar el compte per redirigir certs clients cap a altres serveis i perpetrar l'atac.	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.
AM_6	**Atacants interns maliciosos**	- Apareix una altra capa d'atacants interns, els que gestionen els sistemes dels proveïdors cloud, tot i que s'implementi una segregació de funcions perquè els responsables de la gestió de claus no tinguin accés a l'administració de dades emmagatzemades.	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.
AM_7	**Advanced Persistent Threats (APTs)**	- Quantitat de dades sensibles disponibles al cloud de forma centralitzada.	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.
AM_8	**Pèrdua d'informació**	- El proveïdor de serveis cloud pot esborrar accidentalment les dades. - Desastres naturals que afectin a molts clients degut a la centralització dels serveis cloud.	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.

ID Amenaça	Amenaça	Riscos Addicionals	Probabilitat	Probabilitat	Justificació
AM_9	**Due Diligence insuficient**	- Les estratègies de negoci han de tenir en compte les tecnologies cloud en el seu procés d'avaluació per poder minimitzar el risc i implementar els controls adequats.	N/A	N/A	El propi anàlisi de riscos que s'està realitzant sobre la solució mitigaria l'amenaça de falta de Due Diligence.
AM_10	**Ús abusiu dels serveis cloud**	- Desplegaments de serveis cloud desenvolupats de forma insegura (trials gratuïts, comptes fraudulentes, ...)	N/A	N/A	No aplica donat que Microsoft Azure és un proveïdor cloud contrastat que ofereix mesures de seguretat adients.
AM_11	**Denegació de Servei (DoS)**	- El proveïdor de serveis cloud és un objectiu freqüent ja que engloba diversos serveis i permet realitzar atacs a més d'una organització a la vegada.	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.
AM_12	**Vulnerabilitats amb tecnologia compartida**	- La compartició d'elements d'infraestructura, arquitectura o aplicació, provoca que el compromís d'un sol component de tecnologia compartida exposi a tots els clients i podria arribar a afectar a tot el cloud.	Molt alta	5	Segons CSA, es tracta de les principals amenaces que afecten al cloud, per tant s'entén que la probabilitat d'ocurrència sempre és menor a un any.

6.5. Fase 4: Realització d'un anàlisi del risc inherent

6.5.1. Mètode càlcul risc inherent

Un cop realitzat l'estudi de les amenaces existents i la seva probabilitat d'ocurrència, procedirem al càlcul del risc inherent.

Entenem per risc inherent aquell risc intrínsec que suposa la probabilitat de que es materialitzi una amenaça per l'impacte d'aquesta **sense tenir en compte els possibles controls mitigants**.

El risc inherent, per tant, es calcula com la probabilitat de que es materialitzi una amenaça multiplicat per l'impacte d'aquesta.

$$Risc\ inherent = Probabilitat\ x\ Impacte$$

Per tant, un cop realitzat l'anàlisi de l'impacte (punt 6.3) i amb el catàleg d'amenaces definit juntament amb la seva probabilitat d'ocurrència (punt 6.4), es disposa de tots els elements necessaris per procedir al càlcul del risc inherent.

En primer lloc procedirem a definir l'escala utilitzada pel càlcul del risc, per a fer-ho es defineix primer els 5 nivells de risc a tenir en compte:

Taula 24. Nivells de risc inherent.

Molt baix
Baix
Mitjà
Alt
Molt Alt

A continuació el nivell de risc associat al càlcul de la probabilitat per l'impacte:

Taula 25. Escala pel càlcul del risc inherent.

Impacte						
(5) Molt alt	5	10	15	20	25	
(4) Alt	4	8	12	16	20	
(3) Mitjà	3	6	9	12	15	
(2) Baix	2	4	6	8	10	
(1) Molt baix	1	2	3	4	5	
	(1) Molt baixa	(2) Baixa	(3) Mitjana	(4) Alta	(5) Molt alta	**Probabilitat**

Segons la probabilitat i l'impacte definit i en base a l'escala de colors definida a la Taula 25 es pot concloure que el nivell de risc es mesurarà com s'indica a la següent taula:

Taula 26. Nivell de risc inherent segons la probabilitat i l'impacte..

Nivell de risc	Valor del risc (probabilitat x impacte)
Molt baix	=1
Baix	>1 i <=4
Mitjà	>4 i <=10
Alt	>9 i <=20
Molt Alt	>20

6.5.2. Resultats càlcul risc inherent

Després de realitzar el càlcul del risc inherent s'han obtingut els resultats que es mostren a la Taula 27. A destacar que:

- No s'inclouen les amenaces 9 i 10 perquè, com s'ha comentat en el punt 6.4, aquestes no apliquen per l'anàlisi de la nostra solució.
- L'amenaça de fuga d'informació només afecta a la confidencialitat de la informació que s'ha fugat, però no a la integritat o disponibilitat de la informació continguda en els sistemes de l'entitat. La pèrdua d'informació dins dels sistemes de l'entitat, per contra, sí que afecta a la integritat i disponibilitat de la mateixa.
- L'amenaça de denegació de servei només afecta a la disponibilitat dels sistemes, donat que es tracta d'un atac que té com a objectiu col·lapsar a peticions el servidor víctima de l'atac.

Taula 27. Resultats anàlisi del risc inherent.

			Confidencialitat			Integritat			Disponibilitat		
ID Amenaça	**Amenaça**	**Probabilitat**	**IC**	**RC**	**Risc inherent**	**II**	**RI**	**Risc inherent**	**ID**	**RD**	**Risc inherent**
AM_1	Fuga d'informació	5	3,8	19,2	Alt	N/A	N/A	N/A	N/A	N/A	N/A
AM_2	Pobre gestió d'identitats, credencials i accessos	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
AM_3	APIs no segures	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
AM_4	Vulnerabilitats de sistema i aplicació	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
AM_5	Apropiació indeguda de comptes	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
AM_6	Atacants interns maliciosos	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
AM_7	Advanced Persistent Threats (APTs)	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
AM_8	Pèrdua d'informació	5	N/A	N/A	N/A	3,0	15,0	Alt	4,3	21,7	Molt Alt
AM_11	Denegació de Servei (DoS)	5	N/A	N/A	N/A	N/A	N/A	N/A	4,3	21,7	Molt Alt
AM_12	Vulnerabilitats amb tecnologia compartida	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt

6.6. Fase 5: Identificació del marc de controls a implementar

A continuació s'identificaran tots els controls a implementar per cada una de les amenaces identificades.

Per fer-ho, s'utilitzarà la matriu de controls cloud proposada per Cloud Security Alliance (CSA-CCM (CSA, 2017). El mapeig entre els controls de la CSA – CCM i les diferents amenaces es pot trobar al punt 4.13.2.

Addicionalment, s'assignarà una força a cada un d'ells (baix, mitjà, alt i molt alt), entenent per força el nivell de reducció de risc de cada control. Destacar que només s'estudiarà la implementació dels controls de força alta o molt alta, ja que es considera que són aquells que seran capaços de mitigar el risc de forma suficient.

L'escala que utilitzarem per mostrar el nivell de força és la següent:

Taula 28. Nivells de força.

Baixa
Mitjana
Alta
Molt Alta

Donat que hi ha un elevat número de controls a tenir en compte, no s'inclourà el detall en aquesta memòria. El detall es pot consultar a l'excel adjunt a l'apartat de Recursos. Les conclusions es poden trobar a la Taula 33.

Un cop identificats els controls a tenir en compte i la força de cada un d'ells, es procedirà a fer el càlcul del nivell de cobertura.

6.7. Fase 6: Càlcul del nivell de cobertura

El nivell de cobertura de cada control es calcularà com la força del control per l'efectivitat. L'escala que utilitzarem per mostrar el nivell de cobertura és la següent:

Taula 29. Nivells de cobertura.

Molt Alta
Alta
Mitjana
Baixa

A continuació es mostra com es realitzarà el càlcul del nivell de cobertura segons l'efectivitat i la força de cada un dels controls.

Taula 30. Escala pel càlcul del nivell de cobertura.

Força				
(4) Molt Alta	4	8	12	16
(3) Alta	3	6	9	12
(2) Mitjana	2	4	6	8
(1) Baixa	1	2	3	4
	(1) Baixa	(2) Mitjana	(3) Alta	(4) Molt alta **Efectivitat**

Destacar que cada risc pot ser mitigat per diversos controls. En el cas que un risc tingui més d'un control associat, el nivell de cobertura total es calcularà com la mitjana de tots els nivells de cobertura:

$$nivell\ de\ cobertura\ total\ risc_n = \frac{\sum nivells\ de\ cobertura\ de\ cada\ control\ que\ mitiga\ risc_n}{número\ de\ controls\ que\ afecten\ el\ risc_n}$$

Com en l'apartat anterior, el detall es pot consultar a l'excel adjunt a l'apartat de Recursos. Les conclusions es poden trobar a la Taula 33.

6.8. Fase 7: Càlcul risc residual accés directe a Office365

Entenem per risc residual el nivell de risc que no s'aconsegueix mitigar amb la implementació dels controls mitigants o cobertures.

El risc residual, per tant, es calcula com el risc inherent (intrínsec) que té una organització multiplicat pel nivell de cobertura dels controls de seguretat de la informació implementats.

$$Risc\ residual = risc\ inherent\ x\ nivell\ de\ cobertura$$

Un cop realitzat l'anàlisi de risc inherent (punt 6.5) i avaluat la maduresa del nivell de cobertura dels controls proposats (punt 6.7) es disposa de tots els elements necessaris per procedir al càlcul del risc residual.

En primer lloc procedirem a definir l'escala utilitzada pel càlcul del risc, per a fer-ho es defineix primer els 5 nivells de risc a tenir en compte:

Taula 31. Nivells de risc residual.

Molt baix
Baix
Mitjà
Alt
Molt Alt

A continuació el nivell de risc associat al càlcul del risc inherent per la cobertura:

Taula 32. Escala pel càlcul del risc residual.

Risc inherent					
(5) Molt alt	5	10	15	20	
(4) Alt	4	8	12	16	
(3) Mitjà	3	6	9	12	
(2) Baix	2	4	6	8	
(1) Molt baix	1	2	3	4	
	(1) Baixa	(2) Mitjana	(3) Alta	(4) Molt alta	**Cobertura**

En segon lloc, es procedirà a realitzar el càlcul del risc residual pels dominis identificats. Els resultats obtinguts són els següents:

Taula 33. Càlcul risc residual.

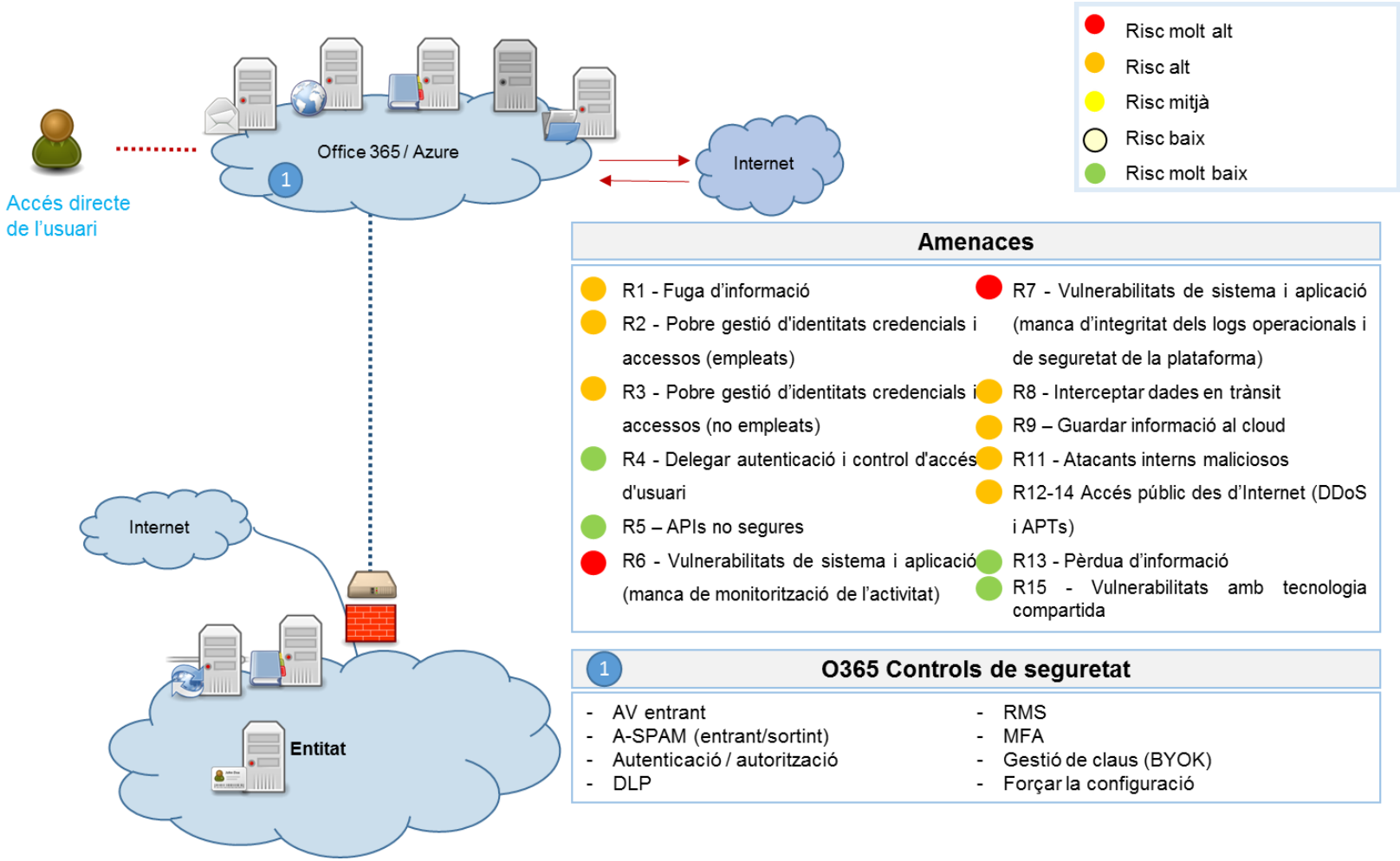
										Confidencialitat		Integritat		Disponibilitat	
ID Amenaça	Risc ID	Risc	ID control	Control	Força control	Efectivitat	Cobertura	Probabilitat		Risc inherent	Risc residual	Risc inherent	Risc residual	Risc inherent	Risc Residual
AM_1	R1	Fuga d'informació	DSI-05	Security mechanisms shall be implemented to prevent data leakage.	Molt Alta	Baixa	Baixa	5		Alt	Alt	N/A	N/A	N/A	N/A
AM_2	R2	Pobre gestió d'identitats credencials i accessos (empleats)	IAM-01 - IAM-13	Identity and Access Management Controls	Molt Alta	Mitjana	Mitjana	5		Alt	Mitjà	Alt	Mitjà	Molt Alt	Alt
AM_2	R3	Pobre gestió d'identitats credencials i accessos (no empleats)	IAM-07	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Molt Alta	Mitjana	Mitjana	5		Alt	Mitjà	Alt	Mitjà	Molt Alt	Alt
AM_2	R4	Delegar autenticació i control d'accés d'usuari	IAM-12	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Molt Alta	Molt Alta	Molt Alta	5		Alt	Molt baix	Alt	Molt baix	Molt Alt	Molt baix

										Confidencialitat		Integritat		Disponibilitat	
ID Amenaça	Risc ID	Risc	ID control	Control	Força control	Efectivitat	Cobertura	Probabilitat		Risc inherent	Risc residual	Risc inherent	Risc residual	Risc inherent	Risc Residual
AM_3	R5	APIs no segures	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Molt Alta	Molt Alta	Molt Alta	5		Alt	Molt baix	Alt	Molt baix	Molt Alt	Molt baix
AM_4	R6	Manca de monitorització de l'activitat	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Molt Alta	Baixa	Baixa	5		Alt	Alt	Alt	Alt	Molt Alt	Molt alt
AM_4	R7	Manca d'integritat dels logs operacionals i de seguretat de la plataforma	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Molt Alta	Baixa	Baixa	5		Alt	Alt	Alt	Alt	Molt Alt	Molt alt
AM_4	R8	Interceptar dades en trànsit	IVS-10	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Molt Alta	Alta	Mitjana	5		Alt	Mitjà	Alt	Mitjà	Molt Alt	Alt
AM_4	R9	Emmagatzetmatge d'informació al cloud	GRM-02 + EKM-04	Encryption & Key Management Storage and Access + Governance and Risk Management Data Focus Risk Assessments	Molt Alta	Mitjana	Mitjana	5		Alt	Mitjà	Alt	Mitjà	Molt Alt	Alt

										Confidencialitat		Integritat		Disponibilitat	
ID Amenaça	Risc ID	Risc	ID control	Control	Força control	Efectivitat	Cobertura	Probabilitat		Risc inherent	Risc residual	Risc inherent	Risc residual	Risc inherent	Risc Residual
AM_5	R10	Apropiació indeguda de comptes	'IAM-01 - IAM-13 + IVS-01	Identity and Access Management Controls + gestió de logs	Molt Alta	Mitjana	Mitjana	5		Alt	Mitjà	Alt	MItjà	Molt Alt	Alt
AM_6	R11	Atacants interns maliciosos	'IAM-01 - IAM-13 + EKM-02-03 + GRM-02	Identity and Access Management Controls + Encryption Key Management + Governance and Risk Management	Molt Alta	Mitjana	Mitjana	5		Alt	Mitjà	Alt	Mitjà	Molt Alt	Alt
AM_7	R12	Accés públic des d'Internet	IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Molt Alta	Mitjana	Mitjana	5		Alt	Mitjà	Alt	Mitjà	Molt Alt	Alt
AM_8	R13	Pèrdua d'informació	BCR-04 - BCR-06 + GRM-02	Business Continuity Management & Operational Resilience	Molt Alta	Molt Alta	Molt Alta	5		N/A	N/A	Alt	Molt baix	Molt Alt	Molt baix

										Confidencialitat		Integritat		Disponibilitat	
ID Amenaça	Risc ID	Risc	ID control	Control	Força control	Efectivitat	Cobertura	Probabilitat		Risc inherent	Risc residual	Risc inherent	Risc residual	Risc inherent	Risc Residual
AM_11	R14	Accés públic des d'Internet	IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Molt Alta	Mitjana	Mitjana	5		N/A	N/A	N/A	N/A	Molt Alt	Alt
AM_12	R15	Vulnerabilitats amb tecnologia compartida	IVS-09	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	Molt Alta	Molt Alta	Molt Alta	5		Alt	Molt baix	Alt	Molt baix	Molt Alt	Molt baix

A sota es mostra una il·lustració amb la solució proposada i el resum de l'anàlisi de riscos realitzat:



Il·lustració 20. Riscos identificats per l'escenari d'accés directe a Office365.

Els principals requeriments que faltarien per complir són:

Taula 34. Resum de compliment dels requeriments.

Domini	ID	Requeriment	Solució Office365
Correu entrant	Req 1	Antivirus i Antispam al perímetre. Tots els correus entrants han de passar per un filtre d'AV i Anti-Spam abans d'arribar al servidor de correu. Allà el correu serà redirigit a la xarxa interna de l'entitat o al servei cloud depenent de l'objectiu.	Compleix
	Req 2	Antivirus i Antispam als servidors de correu. Els servidors de correu han de tenir sistemes d'anti-virus i anti-spam per permetre que el contingut de la bústia sigui escanejat. Idealment, les tecnologies implementades haurien de ser diferents a les utilitzades per protegir el perímetre.	Office365 no ofereix la monitorització constant de les bústies de correu. S'hauria d'implementar una solució tipus CISCO-CES (explicada al punt 3.2.5.3.6) per assegurar el compliment d'aquest requeriment.
	Req 3	Capacitat TLS per les connexions amb tercers.	Compleix
Correu sortint / fuga d'informació	Req 4	Restringir el contingut del correu enviat en base a la mida i el tipus d'adjunt. Contingut actiu a l'adjunt ha d'estar controlat.	El DLP desplegat per Office365 és limitat i s'ha d treballar en la integració amb el DLP corporatiu de l'entitat per poder tenir aquestes funcionalitats.
	Req 5	Anti-virus i anti-spam pel correu sortint	Compleix
	Req 6	Desplegament DLP integrat amb el DLP corporatiu. Aquest ha de permetre la detecció de certes expressions regulars i de contingut indexat en recursos interns.	El DLP desplegat per Office365 és limitat i s'ha de treballar en la integració amb el DLP corporatiu de l'entitat.
Control d'accés i autenticació	Req 7	Requerir l'autenticació segura de l'usuari i la integració amb AD de l'entitat	S'ha d'integrar l'autenticació amb el DA de l'entitat.
	Req 8	Restringir l'accés a les bústies de correu pròpies i autoritzades i tenir un procediment d'accés a altres bústies de correu	Compleix
	Req 9	Limitar els protocols d'accés al correu des de dispositius mòbils o altres dispositius finals, que haurien d'estar securitzats mitjançant una solució MDM	Office365 no ofereix una solució MDM, aquesta s'ha de desplegar a banda i integrar-la amb Office 365.

Domini	ID	Requeriment	Solució Office365
	Req 10	Protegir l'accés web al correu mitjançant encriptació (TLS) i autenticació i restringir l'accés via web al correu electrònic només des de xarxa interna o via la extranet (VPN SSL).	L'accés està protegit via TLS però no hi ha una restricció en l'accés via web perquè la connexió sigui xifrada (VPN SSL).
	Req 11	Monitorització i detecció d'accessos no autoritzats, activitats malicioses o violacions de la política de seguretat de l'entitat.	Les mesures que ofereix Office365 són limitades. Caldria implementar una solució com CASB per millorar el control d'accessos no autoritzats.
Monitorització	Req 12	Assegurar la recol·lecta de logs a diferents capes de la infraestructura a temps real (cada 10 minuts). Incloent els logs dels usuaris administradors.	Compleix
	Req 13	Els logs generats per Microsoft han de tenir el mateix format o s'han de poder integrar amb el SIEM corporatiu de l'entitat.	S'ha de treballar en la integració dels logs proporcionats per Microsoft al SIEM corporatiu de l'entitat per poder fer una correcta gestió d'alertes.
	Req 14	Permetre el servei Journaling amb la mateixa configuració que l'entitat i un període de retenció de 5 anys dins els servidors Exchange d'Office 365 per assegurar que es poden realitzar anàlisis forenses.	S'ha de treballar en la integració dels logs proporcionats per Microsoft al SIEM corporatiu de l'entitat per poder fer una correcta gestió d'alertes.
	Req 15	Tractament dels logs alineats a la política de l'entitat. L'accés ha d'estar restringit, protegit i revisat de forma periòdica.	Compleix
Backup e-mail	Req 16	Aplicar la mateixa política de backup que l'entitat que contempla una retenció de 10 anys, encara que s'acabi la prestació del servei.	S'hauria de veure a nivell contractual. **Out of the scope.**
	Req 17	Restaurar les bústies de correu a temps real.	S'hauria de veure a nivell contractual. **Out of the scope.**
	Req 18	El Reporting del rendiment dels backups ha d'estar sempre disponible.	Compleix
	Req 19	Replicacions de l'Exchange Online per garantir la continuïtat del servei.	Compleix
Encriptació / protecció e-mail	Req 20	Permetre l'encriptació i la signatura electrònica dels correus interns	Les capacitats que ofereix Microsoft són limitades. S'hauria de treballar en la implementació d'una solució com CISCO-CES
	Req 21	Permetre l'encriptació i la signatura electrònica dels correus enviats a direccions externes. Integració amb solucions	Les capacitats que ofereix Microsoft són limitades. S'hauria de treballar en la implementació d'una solució com CISCO-CES

Domini	ID	Requeriment	Solució Office365
		gateway externes encriptades i firmades o enviament d'enllaços al missatge protegit	
	Req 22	Permetre reconèixer correus externs signats electrònicament	Les capacitats que ofereix Microsoft són limitades. S'hauria de treballar en la implementació d'una solució com CISCO-CES
	Req 23	Permetre la gestió de contingut protegit amb DRM tant pels correus entrants com sortints.	Les capacitats que ofereix Microsoft són limitades. S'hauria de treballar en la implementació d'una solució com CISCO-CES
Seguretat Comunicacions	Req 24	Encriptació (TLS) de la comunicació entre el dispositiu de l'usuari i el servidor exchange	Complex
	Req 25	Restringir les connexions a adreces IP de l'entitat	S'hauria d'implementar
Compliance	Req 26	Assegurar l'accés i la possibilitat de realitzar cerques a totes les bústies de correu.	Complex
Migració de dades	Req 27	Permetre exportar dades	Complex
Correus electrònics proveïdors	Req 28	Autenticació DMARC	Les capacitats que ofereix Microsoft són limitades. S'hauria de treballar en la implementació d'una solució com CISCO-CES
	Req 29	Configurar regles pre-definides	Les capacitats que ofereix Microsoft són limitades. S'hauria de treballar en la implementació d'una solució com CISCO-CES

Com es pot veure a la Il·lustració 20 i la Taula 34, amb només la implementació dels controls propis d'Office365 no es dóna compliment als requeriments de l'entitat. Per aquesta raó, en el següent apartat es mostra una proposta amb controls addicionals de seguretat per tal d'intentar mitigar els principals riscos identificats.

6.9. Fase 7: Càlcul risc residual accés directe a Office365 amb controls addicionals de seguretat

En aquest cas es tindran en compte tant els controls propis d'Office 365 com els controls addicionals proposats per fer l'avaluació dels riscos.

Els principals riscos identificats en el punt 6.8 són en relació a la fuga d'informació, l'accés públic d'Office 365 des d'Internet, els atacants interns maliciosos i la manca de monitorització de les activitats realitzades per l'usuaris.

En base a les solucions explicades al punt 3.2.5.3., per tal de mitigar els riscos mencionats al paràgraf anterior, es proposen les següents solucions:

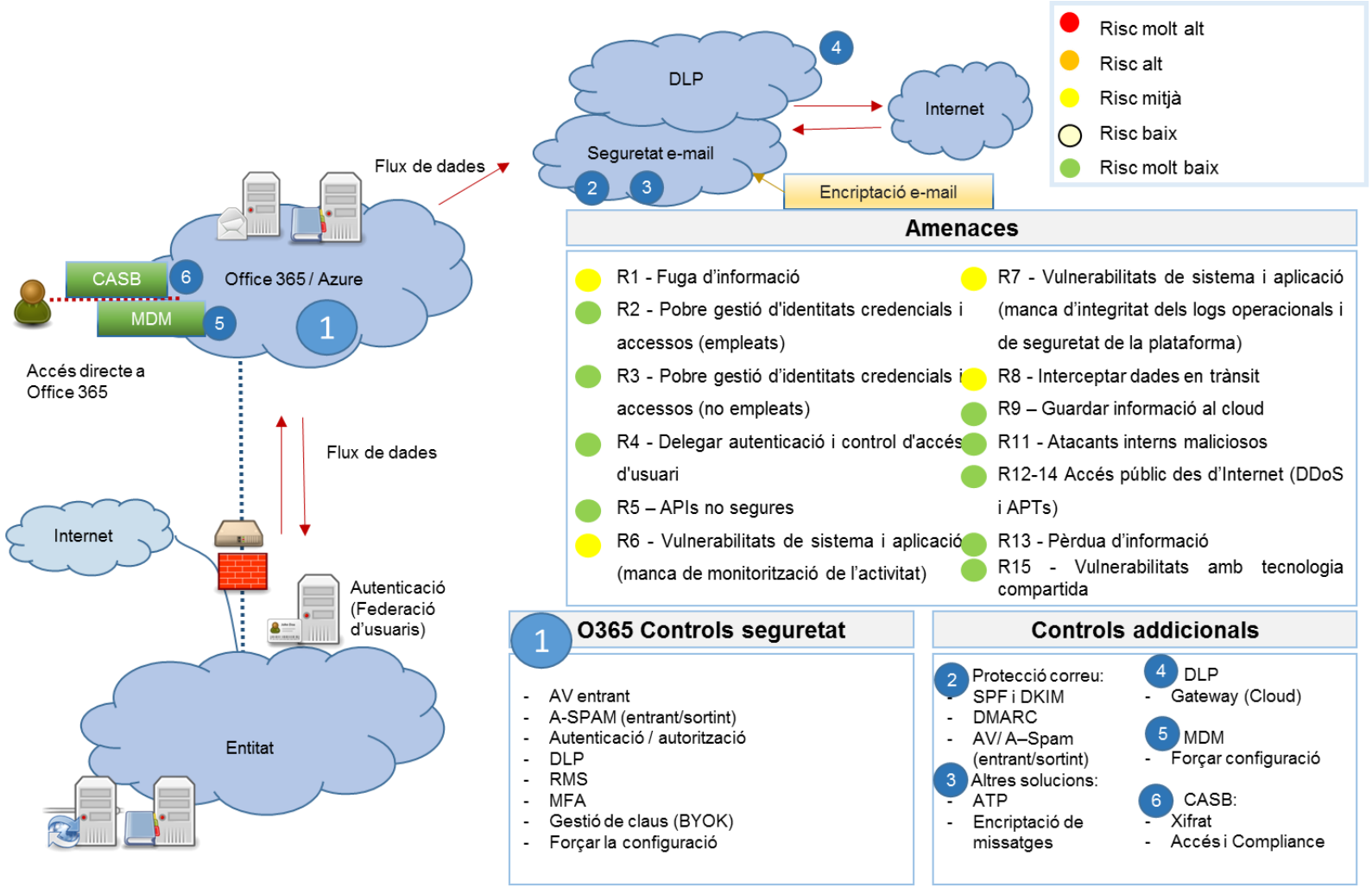
- Implementació d'un CASB (Cloud Access Security Broker) per controlar l'accés directe a Office 365 i guanyar visibilitat de les activitats d'empleat i la implementació de certs controls de detecció i prevenció addicionals. La proposta és utilitzar BlueCoat Elastica.
- Implementació d'una solució MAM (Mobile Application Management) i MDM (Mobile Device Management) per poder tenir un major control sobre la informació emmagatzemada o processada a dispositius personals no confiables.
- Implementació d'una solució de protecció de correu electrònic que proporcioni capacitats d'anti-malware avançades, detecció d'SPAM millorada i amb capacitats de prevenció i de detecció de fuga d'informació (DLP). La proposta és utilitzar el CISCO CES.

Les mesures de seguretat proposades tenen com a objectiu aportar les següents capacitats:

Taula 35. Controls addicionals accés directe a Office365.

Mesures de seguretat	Capacitats
CISCO CES - Protecció de correu	• Filtratge a temps real d'spam i virus. • Autenticació del correu sortint. • Xifrat de correus electrònics. • Compatibilitat amb PGP. • SPK i DKIM. • DMARC.
CISCO CES - ATP (Advanced threat protection)	• Prevenir i detectar proactivament amenaces sofisticades. • Integrar tecnologies de seguretat avançades. • Gestionar una política de seguretat transversalment per tota l'entitat i el cloud. • Incorporar capacitats avançades de resposta a incidents i d'intel·ligència forense.
CISCO CES - Xifrat de missatges	• Enviament de missatges encriptats amb independència de l'adreça de correu electrònic del receptor. • Proporcionar capacitats de xifrat robustes i automàtiques. • Comunicació via TLS.
DLP	• Permet establir polítiques per protegir dades sensibles. • Detecta la informació sensible mitjançant la classificació de missatges i la indexació de documents.
MDM	• Gestió d'un inventari de dispositius. • Gestió de les polítiques a implementar als dispositius. • Monitorització i reporting. • NAC (Network access control). • Gestió de la seguretat als dispositius.
CASB	• Visibilitat de les activitats dels usuaris. • Compliance. • Seguretat de la informació. • Protecció enfront amenaces. • Garantir el control d'accés. • Xifrat cloud.

A la següent il·lustració es pot veure la solució proposada i el resultat de l'anàlisi de riscos tenint en compte els controls addicionals implementats. Com es pot comprovar, el nivell de risc és molt més baix que en l'escenari anterior.



Il·lustració 21.Riscos identificats per l'escenari d'accés directe a Office365 amb controls addicionals

6.10. Fase 7: Càlcul risc residual accés a Office365 mitjançant la xarxa corporativa de l'entitat

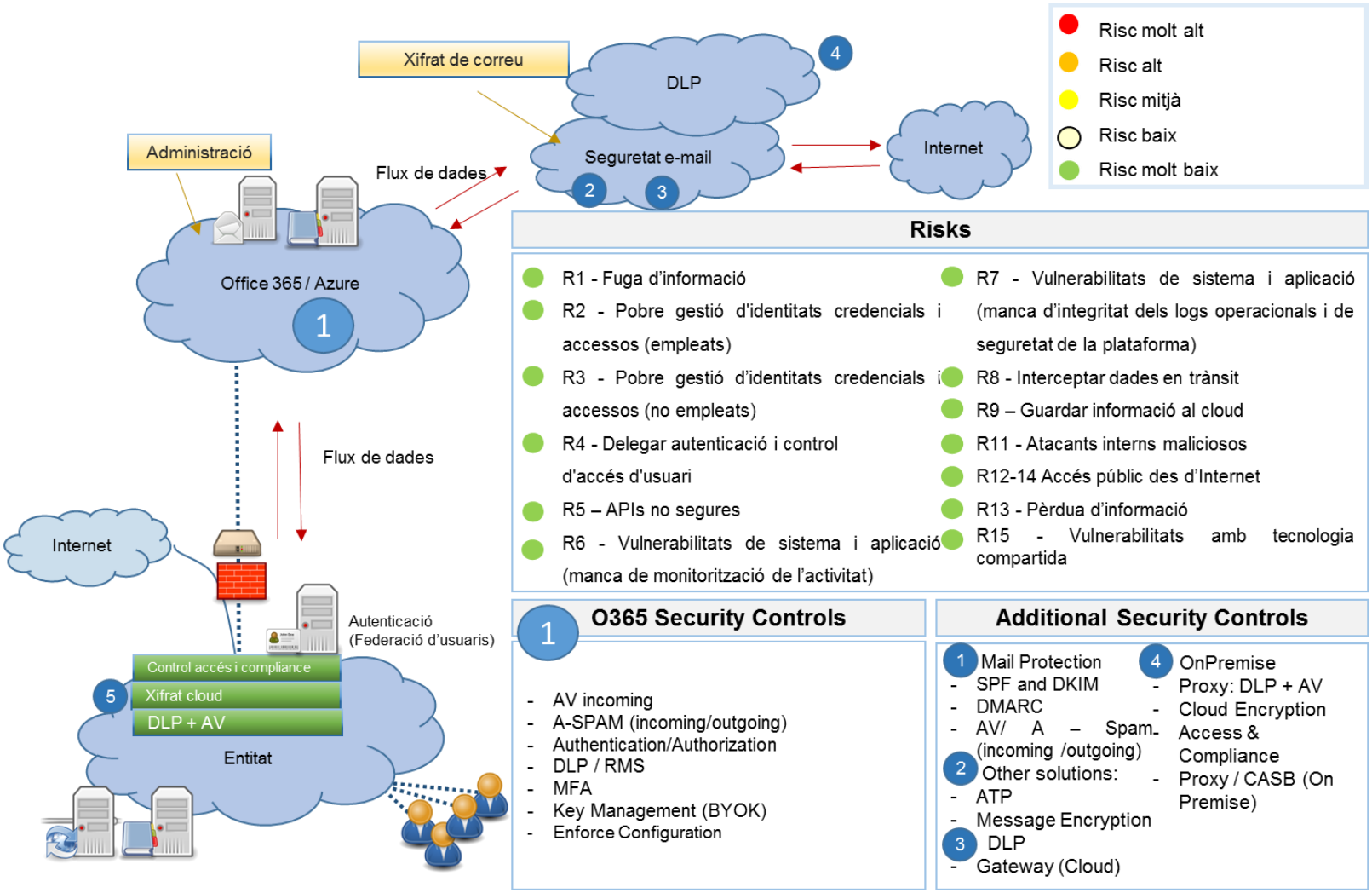
L'altre escenari a analitzar és si l'usuari accedeix al cloud des de la xarxa corporativa de l'entitat. En aquest cas, el nivell de risc hauria de ser més baix ja que s'entén que l'entitat disposa de més mesures de seguretat que poden ajudar a la mitigació d'aquests riscos. Per tal de realitzar l'anàlisi de riscos, suposarem que l'entitat està certificada per la ISO270001 i que per tant disposa de, com a mínim, les següents mesures de seguretat:

Taula 36. Mesures de seguretat pròpies de l'entitat.

Mesures de seguretat pròpies de l'entitat	Capacitats
On-premise DLP	• Permet establir polítiques per protegir dades sensibles. • Detecta la informació sensible mitjançant la classificació de missatges i la indexació de documents.
Anti-malware	• AV/Anti-Spyware/Anti-Malware. • Sandboxing. • ATPs. • Anàlisi del contingut.
On-premise SIEM	• Integració de logs. • Monitorització de logs i gestió de les alertes.
FW / IPS	• Filtratge d'URL. • Xifrat SSL/TLS. • Llista negra de DNS. • URL Reputation – llista negra de webs malicioses (incloent els dominis que ningú hi té accés). • Reporting i Forensic. • Control aplicació web.

Addicionalment, s'entendrà que l'entitat disposa d'un control d'accés (inclosa la federació d'usuaris) i gestió dels usuaris adequada, de processos de patch management i gestió d'Anti-malware i d'una connexió xifrada amb el cloud d'Office365.

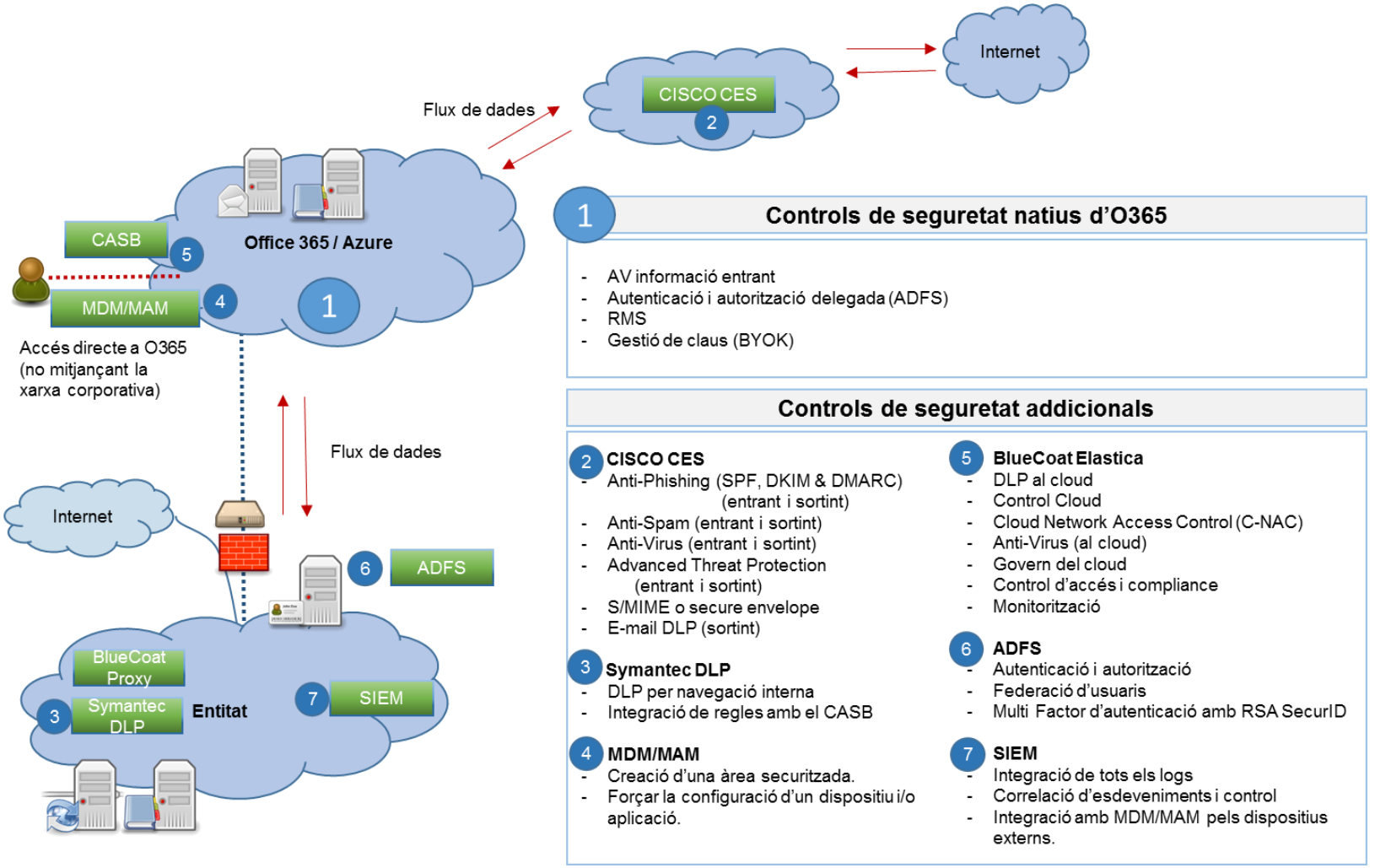
A la següent il·lustració es pot veure la solució proposada i el resultat de l'anàlisi de riscos tenint en compte els controls addicionals implementats. El detall de l'anàlisi de riscos es pot trobar a l'excel adjunt al punt Recursos. Com es pot comprovar, el nivell de risc és encara més baix que en l'escenari anterior.



Il·lustració 22. Riscos identificats per l'escenari d'accés a Office365 mitjançant la xarxa corporativa de l'entitat.

6.11. Solució proposada

En base a la identificació de controls i riscos en els punts anteriors, a continuació es mostra la solució proposada amb les diferents mesures de seguretat addicionals a implementar per tal d'assegurar una correcta mitigació del risc.



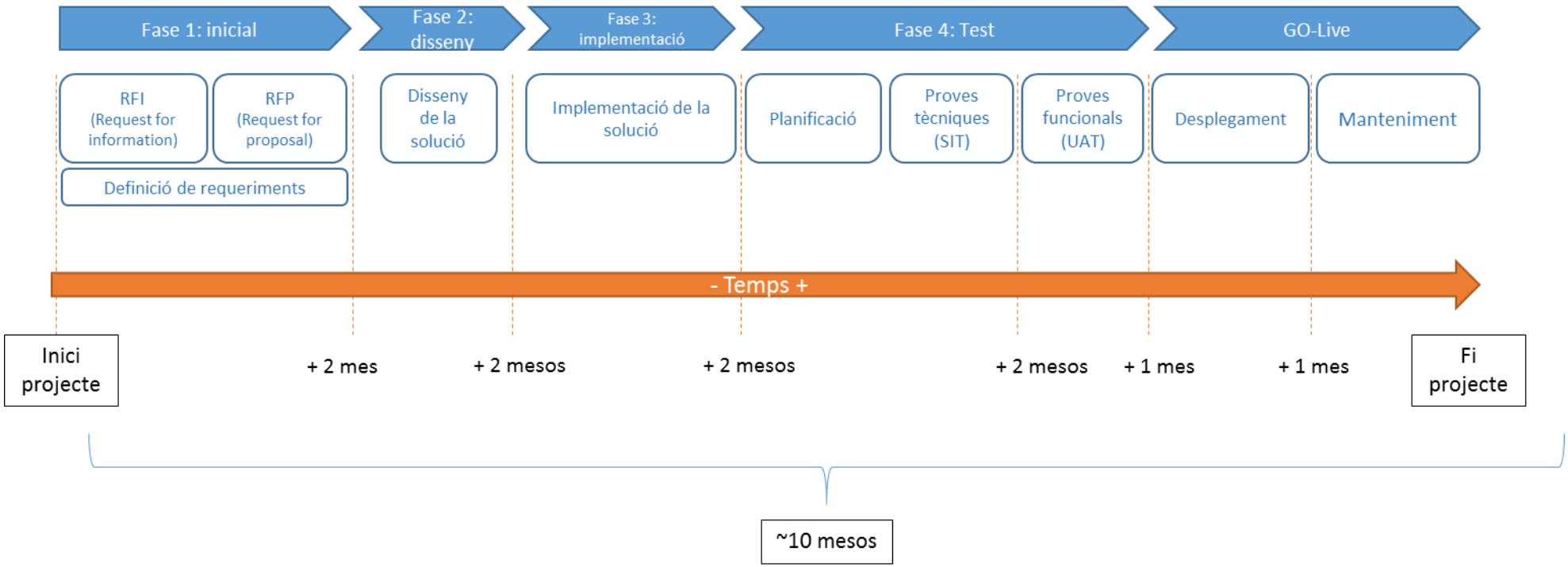
Il·lustració 23. Proposta de securització de la solució.

6.12. Planificació del projecte

Per tal d'implementar la solució proposada en el punt 6.11, se seguirà la planificació mostrada a la Il·lustració 24. Destacar que l'estimació temporal està basada en l'experiència d'implementació de projectes similars i és aproximada. Per realitzar la planificació, s'utilitzarà la metodologia SDLC (Software Development Life Cycle) adaptada a la gestió de projectes:

- **Fase inicial:** en aquesta primera fase s'establiran els primers contactes amb els diferents proveïdors de serveis. Inicialment es recollirà informació per escrit al voltant de les capacitats de diferents proveïdors (RFI). En base a les RFIs, es farà una petició als potencials proveïdors perquè aquests facin una proposta ferma de com ajustarien el seu producte als requeriments indicats per l'entitat (RFP). Un cop finalitzat l'anàlisi de les diferents RFP, se seleccionaran els proveïdors de les diferents mesures de seguretat a implementar.
- **Fase de disseny:** un cop seleccionat el proveïdor, començarà la fase de disseny de la solució en base als requeriments anteriors. És fonamental que el disseny tingui en compte l'arquitectura, infraestructura, comunicacions i la capa d'aplicació de la solució. Incloent la relació amb possibles tercers.
- **Fase d'implementació:** un cop dissenyat, es començarà a desenvolupar / integrar / desplegar segons apliqui el producte per la entitat.
- **Fase de test:** un cop el producte ha estat implementat, caldrà passar per una fase de test abans de la sortida a producció per assegurar que es compleixen tots els requeriments tant tècnics com funcionals. És per això que aquesta fase es dividirà en tres parts:
  - **Planificació:** caldrà planificar els casos d'ús per cada un dels tests i el moment del temps a realitzar-los.
  - **Tests tècnics:** inclouran els test de la part de integració del producte amb la resta d'eines de seguretat. Els encarregats de realitzar-los seran els equips tècnics de desenvolupament o encarregats del desplegament del producte.
  - **Tests funcionals:** inclouran el test de tota la part funcional de l'aplicació. Els realitzaran els usuaris finals de la mateixa.
- **Go-Live**: es tracta de la sortida a producció del projecte. Un cop tots els tests s'hagin completat amb èxit, es procedirà a la pujada a producció i a la popularització de la solució perquè estigui a l'abast de tothom.

A la següent il·lustració es detalla de forma gràfica les diferents fases junt amb els tempos estimats del projecte:



Il·lustració 24. Planificació del projecte.

6.13. Estimació de costos

A continuació es farà una estimació econòmica del cost que suposaria la implementació del projecte. Cal tenir en compte que no es disposa de la informació del cost de cada una de les capacitats de seguretat donat que els proveïdors no faciliten pressupost fins que saben quina és la solució a implementar i el client pel qui l'han d'implementar. Per aquesta raó, s'ha omès el cost de llicenciament i només s'ha tingut en compte la dedicació dels diferents equips de serveis professionals pel desenvolupament del projecte.

El càlcul s'ha realitzat tant a nivell de CAPEX com d'OPEX.

Taula 37. Estimació de costos del projecte.

Capacitat de seguretat	Descripció	CAPEX	Justificació	OPEX	Justificació
Office365	Desplegament i configuració per part d'un equip de serveis professionals de l'eina. S'estima que es destinarà una persona full-time durant 6 mesos.	62.400,00 €	Inclou els serveis professionals utilitzats pel desplegament de l'eina + suport avançat per part del proveïdor (65€/hora)	-	S'hauria d'afegir el cost de llicenciament que es desconeix.
CISCO CES	Desplegament i configuració per part d'un equip de serveis professionals de l'eina. S'estima que es destinarà una persona full-time durant 2 mesos.	20.800,00 €	Inclou els serveis professionals utilitzats pel desplegament de l'eina + suport avançat per part del proveïdor (65€/hora)	-	Gestió de les alertes i manteniment de l'eina per part de l'equip del CSIRT (1 any).
Symantec DLP	Desplegament i configuració per part d'un equip de serveis professionals de l'eina. S'estima que es destinarà una persona full-time durant 2 mesos.	20.800,00 €	Inclou els serveis professionals utilitzats pel desplegament de l'eina + suport avançat per part del proveïdor (65€/hora)	-	Gestió de les alertes i manteniment de l'eina per part de l'equip del CSIRT (1 any).
MDM/MAM	Desplegament i configuració per part d'un equip de serveis professionals de l'eina. S'estima que es destinarà una persona full-time durant 2 mesos.	20.800,00 €	Inclou els serveis professionals utilitzats pel desplegament de l'eina + suport avançat per part del proveïdor (65€/hora)	-	S'hauria d'afegir el cost de llicenciament que es desconeix.

Capacitat de seguretat	Descripció	CAPEX	Justificació	OPEX	Justificació
Bluecoat Elastica (CASB)	Desplegament i configuració per part d'un equip de serveis professionals de l'eina. S'estima que es destinarà una persona full-time durant 2 mesos.	20.800,00 €	Inclou els serveis professionals utilitzats pel desplegament de l'eina + suport avançat per part del proveïdor (65€/hora)	-	S'hauria d'afegir el cost de llicenciament que es desconeix.
ADFS	Desplegament i configuració per part d'un equip de serveis professionals de l'eina. S'estima que es destinarà una persona full-time durant 1 mes.	10.400,00 €	Inclou els serveis professionals utilitzats pel desplegament de l'eina + suport avançat per part del proveïdor (65€/hora)	-	
SIEM	Suposarem que l'entitat ja disposa de l'eina SIEM desplegada i que només haurem de tenir en compte la integració dels logs de les diferents capacitats de seguretat amb l'eina per part d'un equip que ofereix serveis professionals	2.550,00 €	Inclou els serveis professionals utilitzats per la integració de les fonts (85€/font --> 10 servidors * 3 logs per servidor = 30 fonts) + suport avançat per part del proveïdor	-	Gestió de les alertes i manteniment de l'eina per part de l'equip del CSIRT (1 any).
RMS	Desplegament i configuració per part d'un equip de serveis professionals de l'eina. S'estima que es destinarà una persona full-time durant 1 mes.	10.400,00 €	Inclou els serveis professionals utilitzats pel desplegament de l'eina + suport avançat per part del proveïdor (65€/hora)	-	S'hauria d'afegir el cost de llicenciament que es desconeix.
BYOK	Desplegament i configuració per part d'un equip de serveis professionals de l'eina. S'estima que es destinarà una persona full-time durant 1 mes.	10.400,00 €	Inclou els serveis professionals utilitzats pel desplegament de l'eina + suport avançat per part del proveïdor (65€/hora)	-	S'hauria d'afegir el cost de llicenciament que es desconeix.

Capacitat de seguretat	Descripció	CAPEX	Justificació	OPEX	Justificació
Antivirus / Antimalware	Es desplegarà antimalware a tots els servidors de l'entitat. A priori se suposa que els servidors ja existents ja el tenen desplegat. Per tant, pel càlcul de llicències, es farà una estimació que calen 10 servidors per tal de poder acabar de muntar tota la solució proposada.	9.200,00 €	Inclou els serveis professionals utilitzats pel desplegament de l'eina (3 hores per servidor x 10 servidors x 65€/hora) + suport avançat per part del proveïdor (bossa de 100 hores)+ llicència d'ús durant 1 any (75€) x 10 servidors	-	Gestió de les alertes i manteniment de l'eina per part de l'equip del CSIRT (1 any).
CSIRT (Computer Security Incident Response Team)	Gestió per part d'un equip especialitzat en la gestió d'incidents de seguretat reportats per les diferents eines.	-	No aplica durant el desplegament de les eines, és una tasca de l'on-going.	249.600,00 €	Gestió de les alertes i manteniment de l'eina per part de l'equip del CSIRT (1 any). Equip de dues persones, full time, durant 12 mesos a repartir amb les altres eines de seguretat a parts iguals.
Project Manager	Gestió per part d'un equip de dues persones durant 9 mesos per assegurar la integració amb les capacitats de seguretat i la correcta gestió dels proveïdors.	187.200,00 €	Equip de dues persones, full time, durant 9 mesos (= 2880 hores), a 65€/hora.	0,00 €	-
TOTAL		**375.750,00 €**		**249.600,00 €**	

7. Conclusions

En aquest punt s'inclouran les conclusions extretes després de la realització del treball.

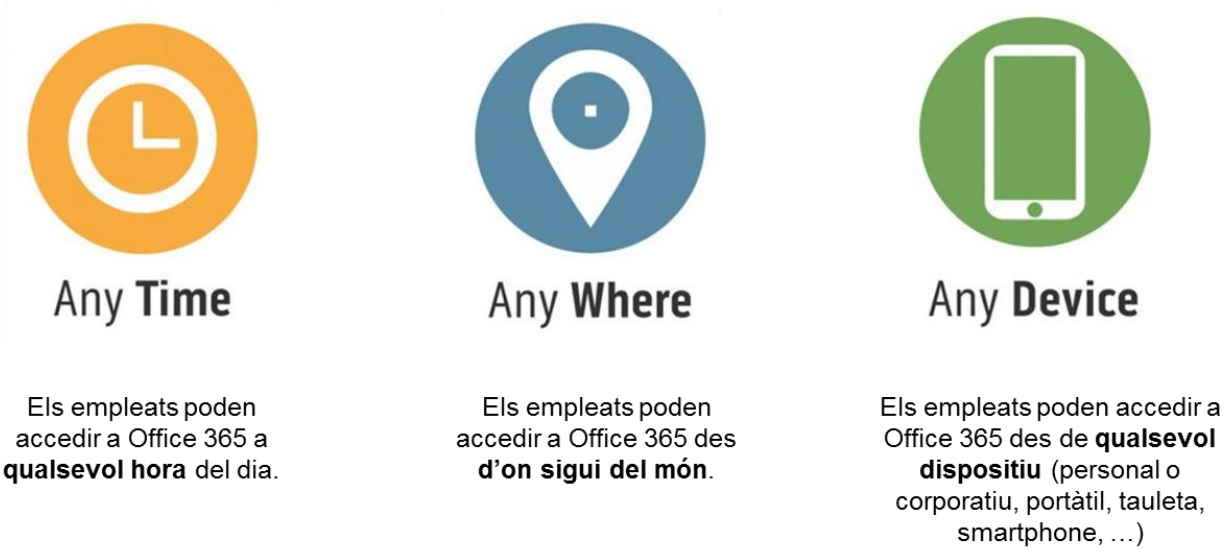
7.1. Valoració del cas pràctic

Durant el cas pràctic, s'han tingut en compte tres escenaris principals:

1. L'accés a Office 365 de forma directa amb els controls natius de Microsoft.
2. L'accés a Office 365 de forma directa amb controls addicionals.
3. L'accés a Office 365 des de la xarxa corporativa de l'entitat.

7.1.1. Valoració escenari 1: accés a Office 365 de forma directa

El fet de poder accedir de forma directa a l'Office365 és el que ofereix un punt diferencial entre les solucions tradicionals on-premise i el cloud, ja que permet accedir al correu corporatiu a qualsevol hora, des d'on sigui del món i des de qualsevol dispositiu (corporatiu o personal, portàtil, tablet, mòbil...).



Il·lustració 25. Característiques solucions cloud.

Però també suposa un major risc ja que s'incrementen les possibilitats de compromís de les dades emmagatzemades al cloud. Fonamentalment, la migració cap a sistemes cloud provoca que l'entitat tingui menys visibilitat sobre:

- Com està gestionant el servei el proveïdor cloud
- Com estan accedint al contingut emmagatzemat al cloud tant els empleats com els proveïdors
- Quines accions es realitzen amb el contingut emmagatzemat al cloud per part d'empleats i proveïdors.

Per mitigar aquests riscos, Microsoft proporciona un nombre de controls natius de seguretat. Segons l'anàlisi realitzat en el punt 6.8, tot i que aquest controls aconsegueixen reduir en certa mesura els riscos, segueix existint un risc residual massa elevat per poder ser acceptat per l'entitat. Els principals gaps detectats són:

- La manca de control via accés directe a l'entorn d'Office 365
- La pèrdua de visibilitat de les activitats dels usuaris

- La manca de securització de les dades emmagatzemades offline o en dispositius personals no segurs
- La detecció i prevenció del malware al correu electrònic
- La tassa de detecció i prevenció d'spam

Per tant, es conclou que només amb la implementació dels controls natius de Microsoft, no n'hi ha prou per garantir la seguretat de la informació al cloud i **no s'aconsella a l'entitat permetre l'accés directe a Office 365**.

7.1.2. Valoració escenari 2: accés a Office 365 de forma directa amb controls addicionals

Donat que l'accés directe és una de les característiques essencials del cloud i la que té més impacte en l'experiència d'usuari, s'ha realitzat l'anàlisi de l'escenari 2. En aquest cas, s'ha avaluat l'accés directe a Office 365 però amb controls addicionals als natius d'Office 365 per tal de mitigar els riscos identificats anteriorment a un nivell acceptable.

En base a l'estudi previ al punt 3.2.5.3, de les capacitats de seguretat aplicables al cloud, s'han proposat els següents controls:

- Implementació d'un cloud security broker (CASB) per controlar la connexió d'accés directe a Office 365. Addicionalment també permetrà guanyar visibilitat de les activitats realitzades pels empleats i la implementació de controls de detecció i prevenció.
- Implementació d'una solució MAM/MDM per garantir un major control de la informació emmagatzemada i/o processada en dispositius personals no confiables.
- Implementació d'una solució de protecció de correu electrònic (CES), que proporciona capacitats avançades d'anti-malware, detecció i prevenció d'spam i detecció i prevenció de fuga d'informació (DLP).

Després de l'anàlisi del punt 6.9, s'ha conclòs **que tenint en compte la implementació tant dels controls natius d'Office 365 com dels controls addicionals proposats, el risc residual de pèrdua o compromís de la informació seria acceptable per l'entitat**. Els principals riscos residuals detectats serien: risc de fuga d'informació, risc d'interceptar dades en trànsit, la manca de monitorització de l'activitat de l'usuari i la manca d'integritat dels logs operacionals i de seguretat de la plataforma.

7.1.3. Valoració escenari 3: accés a Office 365 des de la xarxa corporativa de l'entitat

L'accés via la xarxa corporativa de l'entitat seria un híbrid entre una solució 100% cloud i una solució on-premise. Sí que és veritat que es guanya a nivell d'escalabilitat, reducció de cost i flexibilitat, però no permet oferir una experiència d'usuari millorada respecte la solució ja existent. Tot i això, es tracta de l'opció d'accés més segura ja que permet un major control sobre com els usuaris estan accedint a la informació i les accions realitzades amb el contingut emmagatzemat al cloud (per exemple, evitant dispositius o xarxes no confiables).

Després de l'anàlisi del punt 6.10, si es garanteix l'aplicació dels següents controls:

- On-premise DLP
- Anti-malware
- On-premise SIEM
- FW / IPS
- Control d'accés (inclosa la federació d'usuaris) i gestió dels usuaris adequada

- Processos de patch management i gestió d'anti-malware
- Connexió xifrada amb el cloud d'Office365

Es conclou que **el risc residual de pèrdua o compromís de la informació és acceptable per l'entitat.**

7.1.4. Valoració final del conjunt

A continuació es mostrarà una comparativa dels riscos identificats pels diferents escenaris:

Taula 38. Resum riscos identificats.

Riscos	Accés directe a Office365	Accés directe a Office365 amb controls addicionals	Accés a Office365 mitjançant la xarxa corporativa de l'entitat
R1 - Fuga d'informació	🟠	🟡	🟢
R2 - Pobre gestió d'identitats credencials i accessos (empleats)	🟠	🟢	🟢
R3 - Pobre gestió d'identitats credencials i accessos (no empleats)	🟠	🟢	🟢
R4 - Delegar autenticació i control d'accés d'usuari	🟢	🟢	🟢
R5 – APIs no segures	🟢	🟢	🟢
R6 - Vulnerabilitats de sistema i aplicació (manca de monitorització de l'activitat)	🔴	🟡	🟢
R7 - Vulnerabilitats de sistema i aplicació (manca d'integritat dels logs operacionals i de seguretat de la plataforma)	🔴	🟡	🟢
R8 - Interceptar dades en trànsit	🟠	🟡	🟢
R9 – Guardar informació al cloud	🟠	🟢	🟢
R11 - Atacants interns maliciosos	🟠	🟢	🟢
R12-14 Accés públic des d'Internet (DDoS i APTs)	🟠	🟢	🟢
R13 - Pèrdua d'informació	🟢	🟢	🟢
R15 - Vulnerabilitats amb tecnologia compartida	🟢	🟢	🟢

🔴 Risc molt alt
🟠 Risc alt
🟡 Risc mitjà
⚪ Risc baix
🟢 Risc molt baix

Es pot concloure, doncs, que els proveïdors cloud són capaços d'oferir certes capacitats de seguretat però que encara no són suficients per obtenir una mitigació del risc raonable. Pel que s'han d'afegir controls de seguretat addicionals que permetin assegurar que la solució és segura.

Un cop afegits aquests controls de seguretat, es podria dir que l'empresa està exposada als següents riscos residuals:

Taula 39. Riscos residuals entorn cloud.

Risc	Descripció del risc
Fuga d'informació	Accedint directament a Office365 sense passar per la xarxa corporativa, un empleat intern podria extreure informació als sistemes personals ja que les capacitats del DLP són molt inferiors a les que ofereix una solució on-premise.
Interceptar dades en trànsit	El fet que es pugui accedir a Office365 des de qualsevol xarxa, fins i tot aquelles xarxes considerades com a no segures, fa que existeixi el risc que les dades siguin interceptades en trànsit. Per contra, quan s'assegura que es pot accedir a Office365 mitjançant la xarxa corporativa, aquest risc es veu reduït considerable amb controls de gestió de dispositius finals i de connectivitat dins del propi CPD.
Vulnerabilitats de sistema i aplicació (manca de monitorització de l'activitat)	Donat que els usuaris accediran a la xarxa mitjançant dispositius personals, aquests no es podran monitoritzar mitjançant logs. Addicionalment, tot i que es podrien desplegar solucions MDM i MAM pel control d'aquests dispositius, no és possible assegurar la disponibilitat o integritat dels logs.
Vulnerabilitats de sistema i aplicació (manca d'integritat dels logs operacionals i de seguretat de la plataforma)	

7.2. Comparativa amb la solució On-Premise

L'**objectiu principal** del projecte era analitzar la diferència de nivell de risc de seguretat al què està exposat una empresa del sector financer segons si utilitza una solució cloud o una solució on-premise. Segons comentat en el punt 7.1.4, i en base als resultats que ha obtingut el Miquel Córdoba, company del Màster en Telecomunicacions, en el seu treball, *"Gestió de riscos i anàlisi de la ciberseguretat a l'empresa"* es pot observar que, en la solució de desplegament On-Premise, els principals riscos detectats són:

Taula 40. Riscos residuals On-premise.

Risc	Descripció del risc
Fuga d'informació	Fuga de dades sensibles i informació confidencial a través del correu electrònic. Un usuari intern amb permisos d'administració o no, podria treure informació fora de l'entitat tot i que s'implementin mesures de seguretat via DLP.
Atacs maliciosos	Possibilitat de rebre un atac avançat sobre els sistemes d'informació.

Risc	Descripció del risc
Pèrdua d'informació i de servei	Un atac a gran escala, una catàstrofe natural o un altre conjunt de factors podrien inhabilitar els sistemes i produir una caiguda o una possible pèrdua de dades que afectarien a la disponibilitat de les mateixes.
Errors humans i configuracions incorrectes	Incidents provocats pel factor humà en la gestió de la seguretat de l'entorn i en l'ús del servei per part dels usuaris
Infecció de programari	Possibilitat de ser infectats per programari maliciós

De cara a fer la comparació amb la solució cloud, només es tindran en compte els riscos de nivell mig i aquells que són exclusius d'una de les dues solucions. Ja que es considera que els riscos baixos no són rellevants perquè es troben sota el llindar de risc acceptable establert per l'entitat.

A continuació es mostra una taula resum de la comparativa entre les dues solucions:

Taula 41. Comparativa solució On-premise vs Cloud

Risc	Cloud	On-Prem	Descripció del risc	
			Cloud	**On-Premise**
Fuga d'informació			Accedint directament a Office365 sense passar per la xarxa corporativa, un empleat intern podria extreure informació als sistemes personals ja que les capacitats del DLP són molt inferiors a les que ofereix una solució on-premise.	Un usuari intern amb permisos d'administració o no, podria treure informació fora de l'entitat tot i que s'implementin mesures de seguretat via DLP.
Interceptar dades en trànsit			El fet que es pugui accedir a Office365 des de qualsevol xarxa, fins i tot aquelles xarxes considerades com a no segures, fa que existeixi el risc que les dades siguin interceptades en trànsit. Per contra, quan s'assegura que es pot accedir a Office365 mitjançant la xarxa corporativa, aquest risc es veu reduït considerablement amb controls de gestió de dispositius finals i de connectivitat dins del propi centre de processat de dades.	No aplica en la solució on-premise ja que les comunicacions amb els servidors Exchange es fan a la xarxa interna, on el control sobre la informació és molt més elevat i sí que es pot garantir que sempre sigui xifrat.
Vulnerabilitats de sistema i aplicació (manca de monitorització de l'activitat)			Donat que els usuaris accediran a la xarxa mitjançant dispositius personals, aquests no es podran monitoritzar mitjançant logs. Addicionalment, tot i que es podrien desplegar solucions MDM i MAM pel control d'aquests dispositius, no és possible assegurar la disponibilitat o integritat dels logs.	No aplica ja que s'utilitzaran dispositius coneguts i confiables per accedir al correu electrònic, els quals estaran integrats amb les eines de monitorització de l'entitat.
Vulnerabilitats de sistema i aplicació (manca d'integritat dels logs operacionals i de seguretat de la plataforma)				No aplica ja que qualsevol sistema és gestionat per l'entitat, i per tant la integritat dels logs recau en la correcta gestió dels mateixos i no en un proveïdor extern.
Pèrdua d'informació i de servei			El risc és molt baix a nivell de disponibilitat ja que els proveïdors cloud garanteixen un SLA del 99,9%.	Per garantir una bona disponibilitat del servei, l'arquitectura On-premise requereix el desplegament dels servidors Exchange en dos centres de dades diferents.

Es podria dir, doncs, que els riscos addicionals pel fet d'implementar la solució el cloud serien:

- La intercepció de dades en trànsit
- La manca de monitorització de l'activitat per part de l'usuari i emmagatzematge de la informació offline en dispositius no confiables.
- La manca d'integritat dels logs operacionals i de seguretat de la plataforma

Per contra, ofereix una millor resposta al risc de disponibilitat que sí que afecta a la solució on-premise. Per evitar aquest risc a nivell On-prem, s'hauria de tenir en compte la implementació de servidors d'exchange als dos data centers desplegats amb alta disponibilitat. A nivell de cloud, l'alta disponibilitat te la garanteix el proveïdor amb un SLA del 99,9%.

Per últim, destacar que el principal risc detectat en tots dos casos és el de fuga d'informació. Principalment això és degut a les limitacions que encara presenten les eines de DLP i a la clara dependència que existeix amb la diligència de l'usuari a l'hora d'evitar-les.

Per acabar, doncs, es conclourà que, ja que existeixen les eines de seguretat necessàries per mitigar el risc afegit que suposa tenir els sistemes IT al cloud, la migració cap a sistemes cloud es considera positiva. Dit això, caldrà sempre fer un estudi previ de la solució i analitzar els riscos. El gran error i un dels majors riscos de migrar els sistemes al cloud és suposar que els proveïdors de cloud garantiran totes les mesures de seguretat necessàries i, tal i com s'ha pogut demostrar, no sempre és així.

7.3. Dificultats que hem tingut durant el desenvolupament del projecte

Les principals dificultats a les que ens hem hagut d'enfrontar durant el desenvolupament del projecte ha estat:

- Veure quins controls del marc de controls proporcionat per CSA aplicaven a cada una de les amenaces i com podíem assegurar que amb la implementació d'aquests es garantia la mitigació dels riscos.
- Trobar quines eren les mesures de seguretat incorporades per Microsoft a l'Office365 en base a la documentació de la seva web. Va requerir entendre molt bé la solució que proposaven i documentar-se molt en com Microsoft indicava que es protegir per cada un dels controls proposats per CSA.
- Trobar quines eines i mesures de seguretat calia afegir per tal de poder mitigar els riscos residuals que quedaven implementant només les mesures de seguretat pròpies d'Office365. Va requerir d'una recerca important de les principals eines a tenir en compte per securitzar entorns cloud.

Un cop superats aquests punts, considerem que hem estat capaços de treure uns resultats fiables de la migració a cloud de l'Office365.

7.4. Dedicació al desenvolupament del projecte

La realització del projecte s'ha dividit en 5 grans etapes:

- **Etapa 1 (10 hores)**: Plantejament dels objectius del treball. Etapa curta que va consistir en la conceptualització dels objectius del treball i aprovació del mateix per part del tutor.
- **Etapa 2 (160 hores)**: Recerca d'informació per la realització dels fonaments teòrics i estat de l'art. Es va donar una importància especial en l'estat de l'art per tal de conèixer millor quins eren els riscos a tenir en compte i poder plantejar un cas d'ús que tingués sentit en l'actualitat.

- **Etapa 3 (50 hores):** Plantejament del cas d'ús. Es va treballar en l'abast del cas d'ús, la metodologia a seguir per realitzar-lo i els requeriments a tenir en compte.
- **Etapa 4 (100 hores):** Realització del cas d'ús i extracció de conclusions. S'ha aprofitat la metodologia identificada en l'etapa anterior i s'han extret els resultats dels diferents anàlisis de riscos.
- **Etapa 5 (25 hores):** Comparativa amb la solució On-premise i finalització del treball. Etapa curta, però important, que ha permès extreure les conclusions finals del treball.

Ha estat un projecte al que se li han dedicat un total de **345 hores**. S'ha intentat incloure dins l'abast tots els principals punts a tenir en compte per un professional de la ciberseguretat a l'hora de realitzar un anàlisi de riscos d'una solució per valorar la viabilitat d'implementació de la mateixa.

8. Línies de futur del treball

Les línies de futur del treball passarien per la implementació d'un model de govern del marc de controls definit que permetés la monitorització periòdica dels controls de seguretat amb l'obtenció d'evidències que permetin garantir l'efectivitat dels controls.

Per a realitzar-ho, caldria definir tots els KRIs (Key Risk Indicators), que ens permetran valorar l'efectivitat de cada un dels controls implementats.

Una possible escala per mostrar l'efectivitat és la següent:

Taula 42. Nivells d'efectivitat.

Nivell	Descripció
Molt Alta	El resultat del KRI dóna el valor esperat
Alta	El KRI està un ±10% per sobre o per sota del llindar d'èxit
Mitjana	el KRI està un ±25% per sobre o per sota del llindar d'èxit
Baixa	El resultat del KRI no dóna un valor acceptable o no s'ha pogut medir

Destacar que cada control pot ser mitigat per diversos KRIs. En el cas que un control tingui més d'un KRI associat, el nivell d'efectivitat total es calcularà com la mitjana de tots els nivells d'efectivitat:

$$nivell\ d'efectivitat\ total\ c_n = \frac{\sum nivells\ d'efectivitat\ de\ cada\ KRI\ que\ mitiga\ c_n}{número\ de\ KRI\ que\ afecten\ el\ c_n}$$

Per la monitorització de tots els KRIs definits, es podria utilitzar la següent plantilla:

Taula 43. Seguiment de KRIs.

ID KRI	Actiu	ID + Descripció Control	Força del Control	Descripció KRI	Fórmula de càlcul
Contindrà l'identificador numèric del KRI	Nom de l'actiu sobre el qual es monitoritza el KRI	Descripció i identificador del control mitigant sobre el qual el que es vol mesurar l'efectivitat	Força del control definida al punt 6.6	Descripció del KRI	Formula de càlcul que ens permetrà saber el resultat del KRI

Freqüència	Llindar actual	Resultat KRI	Pla d'acció	Efectivitat KRI
Periodicitat en la que haurem de mesurar el KRI	Llindar definit entre el que es considera que l'efectivitat és bona o dolenta	Resultat d'aplicar la fórmula de càlcul	Si l'efectivitat del KRI és menor a 2, pla d'acció a aplicar per tal de millorar	Valor assignat de l'efectivitat segons definit al punt 6.7

Bibliografia

(ITU), I. T., & Minges, M. (2017). *Global Cybersecurity Index.* Geneva: ITU. Recollit de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

AENOR. (02 / 04 / 2018). Recollit de http://www.aenor.es/aenor/aenor/historia/historia.asp#.WsJUky5uapo

APDCAT. Autoritat Catalana de Protecció de Dades. (2018). *apdcat.gencat.cat*. Consultat el 02 / 04 / 2018, a http://apdcat.gencat.cat/es/documentacio/RGPD/novetats/

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). *NIST Special Publication 800-146. Cloud Computing Synopsis and Recommendations.* Gaithersburg: National Institute of Standards and Techonology (NIST). Consultat el 09 / 04 / 2018

Berry, M. (sense data). Consultat el 10 / 04 / 2018, a http://www.itmanagerdaily.com/cloud-computing-vendors/

Boletín Oficial del estado. (2018). *Protección de Datos de Carácter Personal.* BOE. Recollit de file:///C:/Users/laura.abellanet/Downloads/BOE-055_Proteccion_de_Datos_de_Caracter_Personal.pdf

CCN-CERT. (2017). *Ciberamenazas y tendencias.* CCN-CERT.

CCN-CERT. (2017). *www.ccn-cert.cni.es*. Consultat el 02 / 04 / 2018, a https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/5362-el-2017-acabara-con-mas-de-26-500-ciberincidentes-en-el-sector-publico-y-empresas-estrategicas-espanolas-un-26-mas-que-el-ano-pasado.html

CCN-CERT. (01 / 04 / 2018). Recollit de https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html

CCN-CERT. (2018). Consultat el 02 / 04 / 2018, a www.ccn-cert.cni.es: https://www.ccn-cert.cni.es/ens.html

CEN | CENELEC. (02 / 04 / 2018). *www.cencenelec.eu*. Recollit de https://www.cencenelec.eu/aboutus/Mission/Pages/default.aspx

Chen, T. M. (2004). *The evolution of viruses and worms. Statistical methods in computer security, 1.*

CISCO. (Agost / 2018). Recollit de https://www.cisco.com/c/en/us/products/security/email-security/index.html

CSA. (10 / 03 / 2017). Consultat el 05 / 04 / 2018, a https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

CSA. (2017). *The treacherous 12. Top Threats to Cloud Computing + Industry Insights.* Consultat el 05 / 04 / 2018, a https://cloudsecurityalliance.org/group/top-threats/

CSA. (2018). Consultat el 10 / 04 / 2018, a https://cloudsecurityalliance.org/history/

Cybersecurity. (12 / 03 / 2017). *en.oxforddictionaries.com*. Recollit de https://en.oxforddictionaries.com/definition/cybersecurity

Destefani Neto, M. (18 / 03 / 2014). *IBM*. Consultat el 12 / 04 / 2018, a https://www.ibm.com/blogs/cloud-computing/2014/03/18/a-brief-history-of-cloud-computing-3/

Dignan, L. (14 / 02 / 2018). *ZDNet*. Consultat el 10 / 04 / 2018, a https://www.zdnet.com/article/cloud-providers-ranking-2018-how-aws-microsoft-google-cloud-platform-ibm-cloud-oracle-alibaba-stack/

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (Octubre / 2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* (M. d. Públicas, Editor) Consultat el 05 / 08 / 2018, a https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Encamina. (Agost / 2018). Recollit de https://www.encamina.com/proteccion-informacion-azure-rms-aip/

ENISA. (2009). *Cloud computing. Benefits, risks and recommendations for information security.* Consultat el 11 / 04 / 2018

ENISA. (2018). Consultat el 01 / 04 / 2018, a https://www.enisa.europa.eu/about-enisa

ENISA. (2018). *ENISA Threat Landscape Report 2017 - 15 Top Cyber-Threats and Trends.* ENISA.

ETSI. (02 / 04 / 2018). Recollit de www.etsi.org: http://www.etsi.org/about/what-we-are

Fernandez, M. (14 / 02 / 2018). *Mailfence*. Recollit de https://blog.mailfence.com/es/spf-dkim-y-dmarc-defensa-contra-la-suplantacion-spoofing-en-dominios-personalizados/

Foote, K. D. (22 / 06 / 2017). *DataVersity*. Consultat el 12 / 04 / 2018, a http://www.dataversity.net/brief-history-cloud-computing/

Gartner. (2018). *Forecast: Public Cloud Services, Worldwide, 2015-2021, 2Q17 Update.*

Generalitat de Catalunya. (01 / 04 / 2018). Recollit de https://ciberseguretat.gencat.cat/ca/cesicat/lentitat/

Generalitat de Catalunya. (01 / 04 / 2018). Recollit de https://web.gencat.cat/ca/actualitat/detall/Agencia-de-Ciberseguretat-de-Catalunya-00001

Hechkh, N. (2018). El Reglamento General de Protección de Datos. Fundamentos: Capítulos I a III. Madrid: ISMS.

IBM. (03 / 04 / 2018). Recollit de https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_71/rzarj/rzarjhareqsrecoverytime.htm

Inc, T. (27 / March / Accessed 2018). *techopedia.com*. Recollit de https://www.techopedia.com/definition/31858/watering-hole-attack

INCIBE. (11 / 03 / 2015). *www.incibe.es*. (Instituto nacional de ciberseguridad) Recollit de https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

INCIBE. (2016). *Tendencias en el mercado de la ciberseguridad.* Instituto Nacional de CiberSeguridad. Consultat el 28 / 03 / 2018, a

https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf

INCIBE. (16 / 01 / 2017). *¡Fácil y sencillo! Análisis de riesgos en 6 pasos*. Recollit de https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE. (01 / 04 / 2018). Recollit de https://www.incibe.es/que-es-incibe

ISACA. (2013). *Cobit 5 for Risk.* USA.

ISACA. (2015). *CRISC Review Manual* (6th ed.). USA.

ISACA. (2017). *Cybersecurity Fundamentals Study Guide* (2nd Edition ed.). ISACA.

ISACA, & CSA. (2015). *Cloud Computing Market Maturity.*

ISO. (2005). *UNE-ISO/IEC GUIA 73:2005. Risk management. Vocabulary. Guidelines for use in standards.*

ISO. (2009). *ISO 3100:2009 Risk Management - Principles and Guidelines.* Switzerland.

ISO. (2009). *ISO 31000:2009 Risk Management – Risk Assessment Techniques.* Switzerland.

ISO. (2013). *ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements.* Switzerland.

ISO. (2015). Consultat el 09 / 04 / 2018, a https://www.iso.org/standard/43757.html

Julian, T. (4 / 12 / 2014). Recollit de infosecurity-magazine.com: https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/

Kaspersky Lab. (2017). *IT Security: Cost center or strategic investment? Investigating the new business attitude towards IT security budgets.* Woburn: AO Kaspersky Lab. Consultat el 28 / 03 / 2017, a https://go.kaspersky.com/IT-Security-Economics-Report.html?utm_source=smm_fb&utm_medium=us_fb_o_170920

Khanse, A. (2 / 09 / 2014). Recollit de thewindowsclub.com: http://www.thewindowsclub.com/evolution-of-malware-virus

Lázaro Anguís, F. (2017). Normativa y estándares de referencia de la seguridad de la informació. Madrid: ISMS Forum Spain.

Marlin, S. (21 / 06 / 2017). *TradeWeb*. Recollit de http://www.finregalert.com/fed-official-banks-must-recover-from-cyber-attack-in-two/

Mendoza, Miguel Ángel. (Agost / 2018). Recollit de https://www.welivesecurity.com/la-es/2014/09/24/seguridad-nube-empresas-que-son-casb/

Microsoft. (Agost / 2018). Recollit de https://support.office.com/en-us/article/capabilities-of-built-in-mobile-device-management-for-office-365

Microsoft. (Agost / 2018). Recollit de https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work

Microsoft. (Agost / 2018). Recollit de https://msdn.microsoft.com/en-us/library/bb897402.aspx Consultat l'Agost de 2018

Microsoft corporation. (2015). *Mapping of Cloud Security Alliance Cloud Control Matrix.* Microsoft corporation.

Microsoft Corporation. (28 / 07 / 2018). Recollit de https://products.office.com/en-us/business/office-365-trust-center-security

National Institute of Standards and Technology. (2012). *Generic Risk Model with Key Risk Factors, NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments.* USA.

NIST. (2011). *NIST Special Publications 800-39: Managing Information Security Risks.* USA.

NIST. (2012). *NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments.* USA.

NIST. (May / 2013). (R. Kissel, Ed.) Recollit de Glossary of Key Information Security Term: http://dx.doi.org/10.6028/NIST.IR.7298r2

NIST. (02 / 04 / 2018). Recollit de https://www.nist.gov/cyberframework?AID=1

NSA | CSS. (01 / 04 / 2018). Recollit de https://www.nsa.gov/

PCI Security Standards Council. (02 / 04 / 2018). Recollit de https://www.pcisecuritystandards.org/pci_security/

Ponemon Institute LLC; Accenture. (2017). *Cost of CyberCrime Study. Insights on the security investments that make a difference.* Accenture. Recollit de https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Reglament. (02 / 04 / 2018). Recollit de diec.iec.cat: https://dlc.iec.cat/results.asp?txtentrada=reglament&Submit2=Cerca+directa+al+diccionari

Right Scale. (2018). *State of the Cloud Report. Data to navigate your multi-cloud strategy.*

Rouse, M. (Agost / 2018). Recollit de http://whatis.techtarget.com/definition/BYOE-bring-your-own-encryption

Sherweb. (22 / Febrer / 2018). Recollit de https://www.sherweb.com/blog/mdm-office-365-microsoft-intune/

Thales. (Agost / 2018). Recollit de https://www.thalesesecurity.com/faq/key-secrets-management/what-bring-your-own-key-byok

Trendmicro. (27 / 03 / 2018). *trendmicro.com*. Recollit de https://www.trendmicro.com/vinfo/us/security/definition/Exploit-Kit

UE. (2016). *DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y.* Diario Oficial de la Unión Europea. Recollit de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES

UE. (02 / 04 / 2018). Recollit de http://www.consilium.europa.eu/es/policies/cyber-security/

Union, E. (27 / March / 2018). *eugdpr.org*. Recollit de https://www.eugdpr.org/

Van der Meulen, R., & Pettey, C. (7 / 12 / 2017). (I. Gartner, Editor) Recollit de Gartner Forecasts WorldWide Security Spending will reach $96 billion in 2018, up 8% from 2017: https://www.gartner.com/newsroom/id/3836563

World Economic Forum. (2018). *The Global Risks Report .* Geneva: World Economic Forum. Consultat el 02 / 04 / 2018, a http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Recursos

A continuació s'adjunta l'excel utilitzat per la realització de l'anàlisi de riscos. Dins el mateix excel hi ha una pestanya anomenada *Read me* que indica com es pot navegar per les diferents pestanyes per consultar els resultats obtinguts.