Escola Tècnica Superior d'Enginyeria
Electrònica i Informàtica La Salle

Treball Final de Màster

Màster Universitari en Enginyeria de Telecomunicació

Gestió de riscos i anàlisi de la ciberseguretat a l'empresa

Alumne

Miquel Córdoba Salas

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

Miquel Córdoba Salas

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

Gestió de riscos i anàlisi de la ciberseguretat a l'empresa

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

Resum

Actualment les empreses i organitzacions emmagatzemen quantitats enormes d'informació referent al seu negoci i activitat, dins de sistemes cada cop més complexes gestionats per un gran nombre de persones executant milers de processos. Aquest conjunt de factors fan que sigui necessari estudiar el grau de seguretat sota el que es troba la informació als seus sistemes, per tal d'evitar la pèrdua, modificació, filtració o indisponiblitat d'alguna d'aquesta informació. La tasca fonamental per tal de garantir la seguretat d'un entorn empresarial és conèixer els riscos i amenaces als que aquest entorn s'exposa i un cop identificats, gestionar-los d'una manera eficient.

Aquest treball explica els conceptes fonamentals de la gestió de riscos i la ciberseguretat aplicats a un entorn empresarial. A la primera part s'expliquen aquests conceptes juntament amb les metodologies utilitzades per analitzar el risc d'una organització, les principals amenaces a les que les empreses s'exposen i les eines i capacitats de seguretat que existeixen per mitigar-les. Un cop definits els conceptes descrits, s'ha executat un anàlisi de riscos real aplicat al servei de correu electrònic d'una empresa, una de les eines fonamentals per les organitzacions actuals i que comporta riscos importants per la seguretat de la informació.

L'anàlisi de riscos s'ha aplicat sobre un escenari on-premise, en el que tots els sistemes i recursos de l'organització estan controlats i són propietat de la pròpia empresa, sense comptar amb el servei de proveïdors externs o ni de sistemes externalitzats. Aquest model on-premise dista bastant de la tendència actual de contractar serveis al núvol, que ofereixen més flexibilitat però alhora presenten nous riscos de seguretat per les empreses. Per concloure el treball, s'han comparat els riscos obtinguts a l'anàlisi de la solució on-premise amb els riscos que té una solució al núvol pel mateix tipus de servei de correu electrònic.

Resumen

Actualmente, las empresas y organizaciones almacenan cantidades enormes de información referente a su negocio y actividad, dentro de sistemas cada vez más complejos gestionados por un gran número de personas ejecutando miles de procesos. Este conjunto de factores hacen que sea necesario estudiar el grado de seguridad bajo el que se encuentra la información en sus sistemas, con tal de evitar la pérdida, modificación, filtración o indisponibilidad de alguna de esta información. La tarea fundamental con tal de garantizar la seguridad de un entorno empresarial es conocer los riesgos y amenazas a las que dicho entorno se expone y una vez identificados, gestionarlos de una forma eficaz.

Este trabajo explica los conceptos fundamentales de la gestión de riesgos y la ciberseguridad aplicados a un entorno empresarial. En la primera parte se explican estos conceptos junto con las metodologías utilizadas para analizar el riesgo de una organización, las principales amenazas a las que las empresas se exponen y las herramientas y capacidades de seguridad que existen para mitigarlas. Una vez definidos los conceptos descritos, se ha ejecutado un análisis de riesgos real aplicado al servicio de correo electrónico de una empresa, una de las herramientas fundamentales para las organizaciones actuales y que conlleva riesgos importantes para la seguridad de la información.

El análisis de riesgos se ha realizado sobre un escenario on-premise, en el que todos los sistemas y recursos de la organización están controlados y son propiedad de la propia empresa, sin contar con el servicio de proveedores externos ni de sistemas extrenalizados. Este modelo on-premise se desmarca de la tendencia actual de contratar servicios en la nube, que ofrecen mayor flexibilidad pero a su vez presentan nuevos riesgos de seguridad para las empresas. Para terminar el trabajo, se han comparado los riesgos obtenidos en el análisis de la solución on-premise con los riesgos que tiene una solución en la nube para el mismo tipo de servicio de correo electrónico.

Abstract

Enterprises and organizations nowadays store huge amounts of information related to their business and activity, within complex systems managed by several people who execute thousands of processes. This factors make necessary to study which level of security our systems have in order to prevent the loss, modification, leakage or unavailability of the information. The main task in order to ensure the security of an enterprise environment is to know the risks and threats that affect to this environment and once they have been identified, manage them in an appropriate way.

This paper aims to explain the fundamental concepts of risk management and cybersecurity applied to an enterprise environment. In the first section, those concepts are explained along with the methodologies used to assess risk in an organization, the main threats which enterprises need to face and the security tools and capabilities available to mitigate them. Once those concepts have been defined, a real risk assessment has been performed over an enterprise webmail service, which is one of the most important tools for organizations nowadays and is affected by several risks related to information security.

The risk has been assessed over an on-premise environment, in which all systems and resources of the organization are controlled and are part of the own enterprise, not depending on third party providers or externalized systems. This on-premise model differs from the current trend of contracting and migrating most of the services to the cloud, providing more flexibility but also implying new security risks for data security. Finally, the risks obtained in the on-premise solution have been compared to the ones for the cloud solution for the same kind of webmail service.

Agraïments

Voldria agrair als meus pares el seu esforç en la meva formació durant tota la meva vida i la seva confiança i suport a cadascuna de les etapes que he anat superant, sense la seva empenta res d'això hagués sigut possible.

També al David per trobar en ell a un germà, a un amic i a una persona en qui sempre he pogut confiar.

A la Mónica, per estar sempre al meu costat per treure'm un somriure, per aconsellar.me, entendre'm i animar-me en tot moment.

Agrair també a la meva companya d'aquest treball, la Laura, tot el que m'ha ensenyat des que la conec, el seu consell i la seva ajuda en tot moment. Ha estat un plaer compartir aquest projecte.

Índex

Índex de figures

Índex de taules

1. Introducció

El món de la seguretat informàtica porta experimentant un enorme progrés durant els últims anys, convertint-se sovint en un tema d'actualitat quan es produeixen atacs o fugues d'informació amb repercussió a nivell mundial. Es tracta d'un camp al que porto més d'un any dedicant la meva carrera professional, que m'interessaria conèixer en profunditat i en el que vull seguir formant-me.

És per això que la idea principal a l'hora de començar el projecte era enfocar-lo a la ciberseguretat, la seguretat de la informació i la gestió de riscos. La idea inicial era estudiar un entorn empresarial per tal d'identificar a quines amenaces s'exposa i quins riscos li apliquen a nivell de seguretat. Més enllà d'aquest objectiu principal, s'hauran d'estudiar des dels conceptes bàsics de seguretat, fins a les amenaces més comuns a les que s'exposen les organitzacions i les eines que aquestes tenen a l'abast per mitigar-les.

Un cop definit l'objectiu principal, vam veure amb la Laura Abellanet, companya del Màster en Telecomunicacions, la possibilitat d'ampliar l'abast del projecte i dividir-lo en dues parts:

- La Laura estudiarà la part de securització d'un entorn cloud i es centrarà en els conceptes específics de *Cloud Computing*, en l'estat de la qüestió pel que fa a la computació al núvol i a identificar les principals ciberamenaces que apliquen a aquest paradigma.
- Jo estudiaré un entorn on-premise, controlat íntegrament per la pròpia organització, explicaré els fonaments teòrics bàsics pel món de la ciberseguretat, incloent la descripció de les diferents eines disponibles al mercat per la seva gestió.

Un cop s'analitzi l'entorn on-premise i l'entorn cloud, es compararan els resultats per veure quins riscos derivats comporta cadascun dels dos paradigmes i quines solucions de seguretat són òptimes per a cada cas.

2. Objectius

L'objectiu principal del projecte és **analitzar la diferència de nivell de risc de seguretat** al que 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 tal de poder implementar una solució òptima que permeti garantir un nivell de seguretat adequat i alhora minimitzar el cost a nivell 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 on-premise i en l'altre es realitza el mateix exercici però utilitzant una solució cloud.

En aquest cas, es realitzarà l'anàlisi del nivell de risc de seguretat utilitzant una solució on-premise per al servei de correu corporatiu. Per tal d'assolir aquest 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 on-premise.
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. Introducció a la ciberseguretat

Protegir la informació porta sent una prioritat des de que l'ésser humà ha necessitat mantenir la informació de forma privada i segura, de manera que al llarg de la història, les diferents civilitzacions s'han preocupat de crear mecanismes de xifrat i criptografia, alguns molt simples i d'altres bastant més complexes, per tal de mantenir ocults els seus missatges o secrets.

Actualment i a mesura que la tecnologia avança, també ho ha de fer la seguretat ja que cada cop les empreses i organitzacions emmagatzemen més informació referent al seu negoci i activitat, dins de sistemes cada cop més complexes gestionats per un gran nombre de persones executant milers de processos de manera simultània. Aquest conjunt de factors, i molts d'altres, fan que sigui necessari estudiar el grau de seguretat sota el que es troba la informació als sistemes d'una organització, per tal d'evitar la pèrdua, modificació, filtració o indisponiblitat d'aquesta, cosa que podria portar greus conseqüències.

(ISACA, 2015) La ciberseguretat és la part de la seguretat de la informació que s'encarrega de protegir de les amenaces a les que s'exposa la informació emmagatzemada, processada o transportada a través de sistemes d'informació.

(ISACA, 2015) Per entendre millor la ciberseguretat i la protecció dels actius digitals, s'acostumen a considerar tres conceptes claus per tal de generar polítiques de seguretat:

- Confidencialitat
- Integritat
- Disponibilitat

Els controls de seguretat s'avaluen sovint en funció de com interpreten aquests tres principis, i de manera general, una solució complerta de seguretat hauria de garantir que es compleixen els tres en certa mesura, tot i que la importància de cadascun dependrà dels objectius específics de seguretat de l'organització, els requeriments que se li imposin i les amenaces a les que estigui exposada.

3.1 Confidencialitat

(ISC2, 2015) Un mecanisme de seguretat que ofereix confidencialitat proporciona una garantia de que la seva informació i recursos estan restringits davant d'accessos no autoritzats. En general, per tal de garantir la confidencialitat de la informació a un sistema,

aquesta ha d'estar protegida davant d'accessos, visualitzacions o usos no autoritzats quan està emmagatzemada, en trànsit o sent processada.

Un gran nombre d'atacs es centren en violar la confidencialitat, però els incidents en aquest sentit no només provenen d'atacs intencionats, sinó també d'errors humans, distraccions o ineptituds que poden provocar la revelació d'informació a entitats no autoritzades.

Exemples d'esdeveniments que poden portar a violacions de la confidencialitat poden ser des d'errors al xifrar una transmissió de dades o la no autenticació de sistemes remots abans d'un enviament d'informació, fins a accions generades per errors humans o pel desconeixement de les polítiques de seguretat, com deixar documents confidencials a impressores o no bloquejar l'ordinador al sortir de la oficina.

Algunes contramesures per tal de garantir la confidencialitat davant d'amenaces poden ser el xifrat, el control d'accessos, la classificació d'informació o la formació del personal en matèria de seguretat.

3.2 Integritat

(ISC2, 2015) Per garantir la integritat, els conjunts d'informació o objectes han de mantenir la seva veracitat i poder ésser modificats únicament per usuaris autoritzats. Si un mecanisme ofereix integritat, es garanteix que la informació que conté no ha sigut alterada o modificada respecte al seu estat original.

La integritat es pot estudiar des de tres perspectives diferents:

- Prevenir entitats no autoritzades a realitzar modificacions.
- Prevenir entitats autoritzades a realitzar modificacions no autoritzades.
- Mantenir la consistència interna i externa d'un objecte, per tal de que la seva informació sigui veraç i representi correctament el seu propòsit.

Malgrat que un gran nombre d'atacs es basen en violar la integritat, com passa amb la confidencialitat, aquesta també es pot veure compromesa per errors humans o desconeixements que poden portar a la modificació o eliminació accidental d'informació sensible. Esdeveniments que poden portar a una violació de la integritat poden ser l'esborrat accidental d'un fitxer, l'alteració d'una configuració, la execució de codi maliciós o errors a l'hora d'executar comandes.

Algunes de les contramesures per tal de garantir la integritat poden ser el control d'accessos, els mecanismes de hashing o verificació, els sistemes de detecció d'intrusos o la formació del personal en matèria de seguretat.

3.3 Disponibilitat

(ISC2, 2015) La disponibilitat es centra en garantir que els usuaris autoritzats tindran accés ininterromput a aquella informació per la que tenen permisos. Que un mecanisme de seguretat ofereixi disponibilitat garanteix que els usuaris podran accedir correctament als seus recursos assignats.

Per tal de garantir la disponibilitat d'un sistema, aquest haurà de comptar amb una infraestructura capaç de proporcionar correctament els accessos a usuaris autoritzats i de funcionar ininterrompudament tant en situació normal com en una situació d'incident. D'aquesta manera, s'hauran d'establir controls que garanteixin un acceptable nivell de rendiment, una redundància de sistemes, còpies de seguretat de la informació crítica i sistemes de prevenció davant la pèrdua de dades.

Com passa amb els altres dos principis, la disponibilitat no només es pot veure vulnerada per atacs intencionats, sinó que també pot ser compromesa per errors humans o incidents involuntaris. Alguns esdeveniments que poden comprometre la disponibilitat són l'esborrat accidental de fitxers, errors de hardware i software, incorrecte dimensionament de sistemes i recursos o la indisponiblitat d'instal·lacions.

Algunes de les contramesures per tal de garantir la disponibilitat poden ser la redundància en el disseny i implementació de sistemes, la utilització de sistemes de prevenció d'atacs de denegació de servei, la creació de còpies de seguretat o la existència d'un pla de continuïtat de negoci.

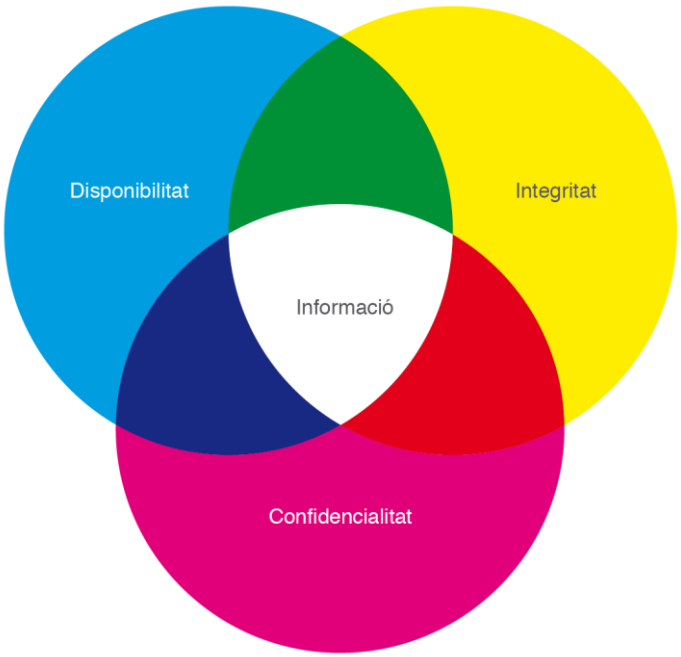

Figura 1. La seguretat com a compromís entre disponibilitat, integritat i confidencialitat (IOC, 2013)

(ISC2, 2015) En general és difícil trobar un sistema que maximitzi les tres propietats. Normalment, i segons el tipus de sistema, se'n prioritzarà alguna. Per exemple, en un sistema que emmagatzemi dades de caràcter policial, l'element que cal prioritzar és la confidencialitat de la informació (és a dir, mantenir el seu caràcter "secret" o confidencial), tot i que també cal tenir molt en compte la preservació (en la mesura que es pugui) de la integritat i la disponibilitat. No serveix de res, per exemple, garantir la confidencialitat mitjançant algun mètode criptogràfic si es permet que un intrús pugui esborrar fàcilment la informació emmagatzemada en el disc dur del servidor (atac contra la integritat). D'altra banda, és absolutament necessari que les dades contingudes en una base de dades policial estiguin disponibles en el decurs d'una actuació policial, per la qual cosa tampoc es pot descuidar la propietat de disponibilitat en un sistema d'aquestes característiques.

En general, cal recordar que un entorn "completament segur" no és possible en el món real i que les polítiques de gestió sempre són un compromís entre el nivell de seguretat que es pot o vol assumir i el cost econòmic que això implica.

3.4 Altres conceptes de seguretat

Addicionalment a aquests tres principis fonamentals també cal destacar-ne d'altres que també val la pena considerar a l'hora de d'implementar una solució de seguretat:

3.4.1 Identificació

(ISC2, 2015) La identificació és el procés mitjançant un subjecte especifica una identitat i s'inicia la seva responsabilitat individual. Quan un individu s'ha identificat i ha estat reconegut, la seva identitat és responsable de qualsevol acció que porti a terme des d'aquell moment.

3.4.2 Autenticació

(ISC2, 2015) El procés de verificar que una identitat reclamada és valida s'anomena autenticació i requereix del subjecte una informació addicional que ha de correspondre exactament amb la identitat indicada. El mètode més comú d'autenticació és la contrasenya, però sovint s'utilitzen segons factors involucrant alguna cosa que l'usuari posseeix (token) o alguna cosa que l'usuari és (empremta del dit o reconeixement facial).

3.4.3 Autorització

(ISC2, 2015) Un cop un usuari s'ha identificat i autenticat, és important tenir en compte que no per això ha de poder accedir a qualsevol recurs d'un entorn o tenir tot tipus de privilegis. És per això que els seus accessos s'han d'autoritzar per tal de que tingui accés únicament a allò que necessiti i que els seus privilegis i drets li permetin executar les funcions assignades a la seva identitat.

3.4.4 Monitorització

(ISC2, 2015) La monitorització permet detectar i portar un seguiment de les accions d'un subjecte autoritzat dins d'un sistema, permetent identificar mals funcionaments, accions malintencionades o comportaments sospitosos. Principalment es basa en guardar registres de les activitats que s'executen dins d'un sistema per posteriorment poder prendre les mesures pertinents.

3.4.5 No repudia

(ISC2, 2015) La no repudia permet assegurar que el subjecte que executa una activitat o esdeveniment no pot negar que aquest esdeveniment ha succeït. Es garanteix utilitzant certificats digitals, identificadors de sessió, logs transaccionals o mecanismes de control d'accés.

4. Riscos i amenaces

La tasca fonamental per tal de garantir la seguretat d'un entorn empresarial és conèixer els riscos i amenaces als que aquest entorn s'exposa i un cop identificats, gestionar-los d'una manera eficient. Una bona gestió de riscos tractarà d'identificar, avaluar i prioritzar els riscos utilitzant de forma coordinada els recursos necessaris per tal de minimitzar i controlar la probabilitat i l'impacte d'un esdeveniment no desitjat.

4.1 Definició

(ISC2, 2015) Entenem com a risc la combinació entre la probabilitat d'un esdeveniment i el seu impacte sobre la nostra organització, mentre que entenem una amenaça com qualsevol esdeveniment que pugui actuar contra algun dels nostres actius i causar un dany o perjudici. Els riscos i amenaces poden tenir diferents tipus de naturalesa i sorgir de fonts molt diverses, com per exemple la incertesa de mercats financers, retards en la planificació dels projectes, causes legals, accidents o robatoris, desastres naturals, atacs deliberats i molts d'altres. En el nostre anàlisi ens centrarem en el ciber risc, que és aquella porció del total de risc que es manifesta dins l'entorn d'informació interconnectada o ciberdomini.

Les empreses actuals es troben a situacions de gran pressió, han de créixer per obtenir un bon rendiment financer i per satisfer als inversors i socis, han d'innovar per seguir creant nous productes i oferir nous serveis per cridar l'atenció dels clients, han de mantenir contents als seus treballadors i formar-los i per a tot això i per moltes altres necessitats, han de mantenir el seu negoci funcionant sense ser interromput per ciberatacs i d'altres incidents de seguretat.

(ISACA, 2016) Avaluar el risc és una acció crítica a una organització moderna. L'efectivitat de les polítiques, les capacitats de seguretat, la ubicació de recursos i la resposta a incidents depenen en gran mesura de l'enteniment de les amenaces a les que l'organització s'exposa, que variaran en gran mesura depenent de factors com el tipus de negoci, la mida, la ubicació, la competència i molts altres factors. Utilitzar un enfocament personalitzat i basat en els riscos per plantejar la estratègia de ciberseguretat permet una presa de decisions més precisa a l'hora de protegir l'organització i una millor utilització del pressupost i dels recursos disponibles. Malgrat això, és molt comú que s'implementin controls sense seguir una avaluació prèvia, donant lloc a que un gran percentatge d'organitzacions actuals no sigui completament conscient de les amenaces a les que s'exposa.

Dins del que anomenem ciber risc, ens trobem una enorme quantitat de factors que poden afectar a la seguretat, com per exemple:

- Complexitat dels sistemes IT
- Diversitat de plataformes, aplicacions i eines utilitzades
- Utilització de sistemes on-premise, cloud o híbrids
- Necessitat de suport per part de proveïdors externs
- Tipus d'informació gestionada
- Recursos humans i infraestructures utilitzades

Malgrat que és complicat predir quins riscos associats ens generaran cadascun d'aquests factors, l'organització haurà d'anticipar-se de forma eficient i raonable per tal de poder-se anticipar i reaccionar davant de les situacions que aquests riscos puguin produir.

4.2 Principals riscos i amenaces actuals

Vivim en una època on tot està connectat, hi ha més dispositius que mai, en que s'utilitzen milers de serveis digitals diferents i en que cada cop les nostres dades s'utilitzen a més llocs i per a més tipus de tractaments. La informació al ciberespai s'ha convertit en un actiu d'enorme valor per a moltes empreses i en conseqüència un objectiu principal per aquells que n'hi vulguin provocar danys.

(Ana Daiscalescu/Heimdal, 2018) L'avanç de la tecnologia, el fàcil accés a plataformes digitals i l'aparent anonimat dels usuaris a la xarxa ha portat a que constantment apareguin noves amenaces i a centenars de milions de ciberatacs diaris. D'entre les principals amenaces actuals podem destacar:

- **Ciberespionatge industrial**
  (Ana Daiscalescu/Heimdal, 2018) Robatori d'informació a empreses amb l'objectiu d'accedir a les seves dades i informació més valuosa (propietat intel·lectual, desenvolupaments tecnològics, estratègies d'actuació, bases de dades de clients, etc).

- **Atacs a infraestructures crítiques**
  (Ana Daiscalescu/Heimdal, 2018) Els atacs a infraestructures crítiques (centrals elèctriques i nuclears, plantes d'aigua, aeroports o hospitals) no deixen d'augmentar i el seu volum s'ha multiplicat per set en els últims dos anys. Els atacs amb software

maliciós són els més comuns tot i que aquests tipus d'infraestructures també solen ser objectiu d'atacs de denegació de servei i d'accessos no autoritzats.

- **Cibermercenaris**

  (Ana Daiscalescu/Heimdal, 2018) Formats per grups criminals amb coneixements avançats, aquestes organitzacions són contractades per tal de desenvolupar atacs dirigits contra objectius concrets i amb motivacions molt diverses (polítiques, econòmiques, per reputació i reconeixement, etc).

- **Atacs contra serveis financers**

  (Ana Daiscalescu/Heimdal, 2018) Els atacs amb software específicament dissenyat per extreure dades de targetes de crèdit i cada cop més, centrats en els dispositius mòbils. Sovint el grau de sofisticació d'aquest programari maliciós indica una gran organització criminal, amb grans inversions de desenvolupament i moltes hores d'elaboració.

- **Ciberdelincuents organitzats**

  (Ana Daiscalescu/Heimdal, 2018) Màfies i grups criminals que han traslladat al món virtual les seves accions al món real. Frau online, clonació de targetes de crèdit, extorsió, blanqueig de capitals, etc.

- **Ciberactivistes**

  (Ana Daiscalescu/Heimdal, 2018) Persones o grups que, moguts per alguna ideologia, busquen destruir l'estructura i organització d'una empresa, sovint utilitzant atacs de denegació de servei, la desfiguració de pàgines web o la publicació de dades compromeses.

És per totes aquestes amenaces conegudes, per moltes d'altres existents i per d'altres encara per sorgir, que cada cop és més important que les empreses mantinguin un control exhaustiu sobre la seguretat de la seva informació i dels seus actius crítics, així com que analitzin els riscos als que s'exposen i apliquin les polítiques adequades.

4.3 Polítiques

(ISACA, 2015) Les polítiques de seguretat són l'element principal de la ciberseguretat i la governança general de seguretat. Aquestes especifiquen els requeriments i defineixen els rols i les responsabilitats de tots els integrants d'una organització, així com els comportaments i actuacions esperades en funció de la situació. Per tant, han de ser creades, acceptades i validades per l'alta direcció abans de ser comunicades a la resta d'integrants de l'organització. Durant aquest procés, es poden donar situacions on s'hagin de crear documents per referir-se o detallar situacions particulars, separades del gruix principal de l'organització, especialment quan aquesta tingui regulacions específiques per protegir certs tipus d'informació.

(ISACA, 2015) Tot document d'aquesta naturalesa ha de seguir el procés formal de ser creat, revisat, actualitzat i aprovat com a mínim un cop a l'any. Addicionalment, es pot donar la necessitat d'aplicar una excepció dins d'una certa política, la qual és una situació que es pot originar per motius de negoci, de processos interns, casuístiques particulars, etc. I que per tant provocarà que s'hagi de definir un procés inequívoc per aprovar excepcions per part de la direcció de l'organització i per monitoritzar aquestes excepcions durant el seu cicle de vida.

(ISACA, 2015) El nombre i el tipus de polítiques que una organització decideix implementar varia en funció de la seva mida, cultura i complexitat. La majoria d'empreses petites o mitjanes disposen d'una política general d'alt nivell sobre seguretat que serveix com a fonament per altres documents de compliment i governança, mentre que a organitzacions més grans és més comú subdividir les polítiques dins de diferents àmbits per tal de garantir la seguretat de la informació a les diferents àrees, operacions, procediments i entorns.

4.4 Controls

(ISACA 2015) La ciberseguretat és un entorn dinàmic i en constant canvi que requereix una monitorització continua i una actualització i comprovació de la seva efectivitat periòdiques a la vegada que la tecnologia i el negoci evolucionen. Aquesta monitorització es du a terme mitjançant controls, els quals són crítics per mantenir la seguretat dins de la infraestructura tecnològica d'una organització i la manca d'aquests o els error al implementar-los són una de les principals causes d'incidents de seguretat dins de les empreses.

(Linda McGlasson, 2009) De controls aplicables a la ciberseguretat n'hi ha de moltes menes i varietats, amb objectius molt diversos i amb un impacte diferent sobre l'organització. Entre els més comuns podem trobar els següents:

- Inventaris del hardware autoritzat i no autoritzat
- Inventaris del software autoritzat i no autoritzat
- Configuracions segures de hardware i software
- Manteniment i anàlisi dels logs de seguretat
- Software de seguretat per aplicacions
- Utilització controlada dels accessos privilegiats
- Gestió d'usuaris i d'identitats
- Identificació i resolució continua de vulnerabilitats
- Programari específic de seguretat per a xarxa, dispositius i aplicacions
- Limitació i control de ports, protocols i serveis
- Controls de dispositius sense fils
- Protecció davant la fuga d'informació
- Capacitats de resposta davant d'incidents
- Capacitats de resposta davant desastres
- Conscienciació i formació sobre seguretat

Tot i que aquest pot ser un resum dels controls més comuns, una organització no pot basar la seva política de seguretat en complir directament aquestes directives sense haver elaborat prèviament un anàlisi de riscos ja que segons la seva naturalesa, el seu tipus de negoci, la seva mida o la seva situació al mercat, pot necessitar d'altres tipus de controls o haver-ne d'implementar algun dels descrits anteriorment sota una perspectiva diferent i adequada a les seves necessitats.

(ISC2, 2015) Els controls de seguretat han d'aportar beneficis que siguin mesurables i monitoritzables. Si els resultats d'un control no es poden quantificar, mesurar, avaluar o comparar, llavors no aporta realment cap seguretat. De tota manera, mesurar la efectivitat d'un control no acostuma a ser un valor absolut, sinó que molts d'ells en comptes de valors específics com el nombre d'atacs evitats o el nombre d'accessos no autoritzats, aporten graus de millora o resums generals de situació.

4.5 Anàlisi de riscos

4.5.1 Conceptes clau

(ISC2, 2015) La gestió del risc utilitza una àmplia terminologia que ha de ser clarament entesa per tal de saber del que s'està parlant. Ja s'han definit els conceptes de risc i vulnerabilitat anteriorment, però n'existeixen d'altres que sortiran constantment durant l'anàlisi:

Actiu Qualsevol cosa (informació, persona, material, instal·lació, sistema, programa...) que val la pena protegir dins del nostre entorn. Cal considerar com a actiu qualsevol cosa sota el control d'una organització a la qual aquesta li hagi donat un valor.

Vulnerabilitat Es defineix com a vulnerabilitat a la debilitat d'un actiu o la manca o debilitat d'una salvaguarda. En altres paraules, una vulnerabilitat és un error, descuit, fragilitat, limitació, o susceptibilitat de la infraestructura IT d'una organització. Si una vulnerabilitat s'explota es poden provocar danys o pèrdues en els actius de l'empresa.

Exposició L'exposició és el fet de ser susceptible a la pèrdua o el dany a un actiu a causa d'una amenaça. Un alt nivell d'exposició no implica que una amenaça es vagi a materialitzar, simplement vol dir que existeix una vulnerabilitat i una amenaça que podria explotar-la.

Salvaguarda Una salvaguarda o control és qualsevol cosa que elimina o mitiga una vulnerabilitat o protegeix contra una o varies amenaces. Pot ser per exemple la instal·lació d'una nova versió de software, un canvi de configuració, la contractació de guàrdies de seguretat o la millora de les polítiques de seguretat.

Atac Un atac és la explotació d'una vulnerabilitat per part d'una amenaça, per tant és qualsevol intent intencionat d'explotar una vulnerabilitat per tal de danyar els actius d'una organització.

Un cop definits tots aquests conceptes, és podria dir que el risc es mitiga amb salvaguardes, que s'utilitzen per protegir actius que es troben en perill a causa de les amenaces. Aquestes amenaces exploten vulnerabilitats, cosa que resulta en una exposició que genera un risc.

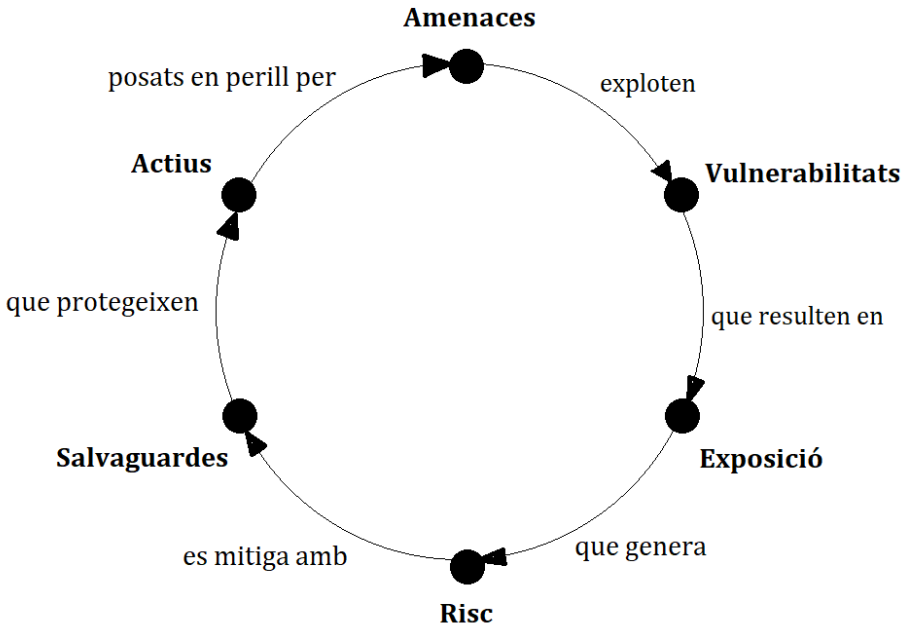

Figura 2. Relacions entre els principals conceptes de l'anàlisi de riscos (ISC2, 2015)

4.5.2 Metodologies

(ISACA, 2015) Tot i que cada metodologia per a realitzar un anàlisi de riscos pot presentar diferents solucions i maneres d'abordar el problema, la majoria contemplen tres accions principals:

- Identificació d'actius
- Anàlisi d'amenaces
- Anàlisi de vulnerabilitats

Aquest procés comença examinant les fonts de risc (amenaces i vulnerabilitats) per conèixer el seu impacte i les seves conseqüències. Un cop analitzats tots aquests atributs, el risc es pot classificar segons la seva probabilitat i el seu impacte.

(ISC2, 2015) És important recordar que tots els sistemes IT tenen risc i que no hi ha cap manera d'eliminar el cent per cent del risc. Per tant, l'alta direcció d'una organització serà responsable de decidir quins riscos són acceptables i quins no. Per tal de dur a terme aquesta elecció, és important comptar amb un anàlisi de riscos detallat.

Quan s'elabora un llistat d'amenaces, s'ha d'avaluar individualment cadascuna de les amenaces i el seu risc associat. Principalment, existeixen dues metodologies principals per

fer un anàlisi de riscos: quantitativa i qualitativa, tot i que sovint es combinen ja que els dos mètodes són importants per abordar el risc de manera correcta.

(ISC2, 2015) L'anàlisi quantitatiu genera percentatges de probabilitat concrets, generant com a resultat final un informe que dona valors concrets als actius, a la probabilitat de pèrdua, al cost de les salvaguardes i al seu valor. Malgrat que aquest tipus d'informe és fàcil d'entendre per qualsevol acostumat a aquest format, no és suficient amb l'anàlisi quantitatiu ja que no tots els elements i factors de l'anàlisi es poden quantificar ja que molts són qualitatius, intangibles o subjectius. És per això que també s'utilitza l'anàlisi qualitatiu, que no es basa tant en els càlculs i les xifres concretes sinó en categoritzar les amenaces segons una escala definida per tal d'avaluar el seu risc. Existeixen diferents tècniques per tal d'analitzar el risc qualitativament, tals com la tècnica de Delphi, l'anàlisi d'escenaris o mètodes més comuns en altres camps com les pluges d'idees, els qüestionaris o les entrevistes.

Característiques	Quantitatiu	Qualitatiu
Utilitza funcions complexes	Si	No
Utilitza un anàlisi cost/benefici	Si	No
Proporciona resultats específics	Si	No
Requereix treballar amb suposicions	No	Si
Permet l'automatització	Si	No
Utilitza una gran quantitat d'informació	Si	No
És objectiu	Si	No
Utilitza opinions	No	Si
Ofereix resultats rellevants	Si	Si

Taula 1. Diferències entre l'anàlisi quantitatiu i qualitatiu (ISC2, 2015)

(ISC2, 2015) El resultat de l'anàlisi consistirà en diferents entregables, entre els que podem destacar:

- La valoració detallada de tots els actius de l'organització.
- Un llistat exhaustiu de les amenaces, riscos, probabilitats i impactes.
- Un inventari de les salvaguardes específiques per a cada amenaça.
- Un anàlisi del cost i benefici de cada salvaguarda.

Aquesta informació és essencial per l'alta direcció de l'organització ja que és en la que es basaran per prendre decisions sobre les salvaguardes a implementar i les modificacions

sobre les polítiques de seguretat. Respecte al risc, existeixen quatre possibles accions o respostes:

Reduir-lo o mitigar-lo (ISC2, 2015) La reducció o mitigació del risc es produeix al implementar salvaguardes o mesures que eliminin vulnerabilitats i bloquegin les amenaces. Escollir la mesura més adequada tenint en compte el cost i el benefici és una part important de la gestió de riscos però no pas de l'anàlisi de riscos. Una altra manera de reduir el risc és eliminant la seva font o causa, per exemple deixar d'utilitzar un protocol amb vulnerabilitats o allunyar les nostres instal·lacions de mars o rius per evitar el risc d'inundació.

Assignar-lo o transferir-lo (ISC2, 2015) Una manera alternativa de gestionar el risc és carregar el possible cost del dany o pèrdua d'un actiu sobre una altra entitat, per exemple contractant una assegurança que cobreixi les possibles pèrdues o mitjançant la externalització.

Acceptar-lo (ISC2, 2015) Acceptar el risc és la decisió que pren l'alta direcció d'una organització després d'avaluar que el cost de les salvaguardes necessàries per mitigar-lo (ja sigui pensant en diners, esforç, temps o d'altres) és superior al cost dels danys o pèrdues que pot suposar. També vol dir que la gerència de l'empresa ha decidit acceptar les conseqüències i les pèrdues si el risc es materialitza. En la majoria de casos, acceptar el risc suposarà la creació d'un document detallant els motius de la decisió, el responsable d'aquesta i qui es farà càrrec de les pèrdues si el risc es materialitza.

La decisió d'una organització sobre acceptar un risc es basa en la seva tolerància al risc, que és la capacitat d'una organització d'absorbir les pèrdues generades i associades a un risc.

Rebutjar-lo o ignorar-lo (ISC2, 2015) Mentre que les tres anteriors decisions son vàlides i totes elles es prenen a les organitzacions reals, la decisió de rebutjar, ignorar o negar l'existència d'un risc real és inacceptable. D'aquesta manera es confia en que mai es materialitzarà, donant lloc a una situació d'imprudència i una clara exposició a les amenaces existents.

4.5.3 Selecció de salvaguardes

(ISC2, 2015) La selecció de salvaguardes, controls o mesures de seguretat per mitigar els riscos derivats de l'anàlisi es basa en el resultat d'analitzar el cost i el benefici que genera cadascuna d'aquestes, tenint en compte també els següents principis bàsics:

- El cost de la salvaguarda o control ha de ser menor que cost de l'actiu al que protegeix i que el benefici que aporta.
- El resultat de l'aplicació ha de provocar que el cost d'un atac per part d'un subjecte sigui superior al benefici que pugui extreure'n.
- Les salvaguardes han d'aportar solucions a problemes reals i identificats. És comú que les organitzacions adquireixin solucions de seguretat simplement perquè són populars, innovadores o perquè algú els hi ha aconsellat, sense haver-se parat abans a pensar si realment són necessàries o si aportaran un benefici superior al cost (sovint elevat) que impliquen.
- Els beneficis d'una salvaguarda han de ser provables, verificables i no han de presentar dependències entre elles per tal d'evitar errors en cascada. També han d'aportar una protecció uniforme i consistent per a tots els usuaris, sistemes i protocols.
- Les salvaguardes han de requerir la mínima intervenció humana després de la posada en marxa i la configuració inicial. També han de gestionar correctament la seva accessibilitat i els seus privilegis.

5. Normatives existents en seguretat de la informació

Avui en dia la seguretat de la informació és un aspecte clau tant per les empreses com per als seus clients, ja que la manipulació, filtració o destrucció de dades sensibles pot tenir conseqüències irreparables i de gran impacte en funció del tipus d'informació compromesa. És per això que des de governs i grups industrials s'han creat múltiples marcs regulatoris, normatives i estàndards per garantir que les empreses que tracten dades sensibles compleixen amb certs requisits i tenen certa maduresa a nivell de seguretat.

D'aquestes normatives i estàndards n'hi ha de molts tipus i creats per fonts diverses amb diferents finalitats, a continuació es descriuen alguns dels més coneguts:

5.1 ISO/IEC 27001

(AENOR, 2016) Es tracta d'un estàndard internacional per la seguretat de la informació aprovat i publicat a l'octubre de 2005 per la Organització Internacional per la Estandardització i per la Comissió Internacional d'Electrotècnia. Especifica els requeriments per establir, implementar, mantenir i millorar de forma continua el sistema de gestió de la seguretat de la informació en el context d'una organització i inclou requeriments per l'anàlisi i tractament de riscos. Entre les activitats a desenvolupar quan s'implementa la ISO 27001 podem trobar:

- Definició de l'abast del sistema de gestió i seguretat de la informació.
- Definició d'una política de seguretat.
- Definició d'una metodologia i criteris d'anàlisi i gestió de riscos.
- Identificació de riscos.
- Avaluació de controls a implementar, aplicabilitat i requeriments.
- Definició de mètriques i indicadors de l'eficiència dels controls.
- Desenvolupament de programes de formació i conscienciació en seguretat de la informació.
- Gestió de recursos i operacions.
- Gestió d'incidències.
- Elaboració de procediments i documentació associada.

La ISO 27001 pot ser implementada a qualsevol tipus d'organització, amb o sense ànim de lucre, privada o pública i permet que aquesta sigui certificada per una entitat independent conforme la compleix.

5.2 NIST 800

Les sèries NIST 800 són un conjunt de documents que descriuen les polítiques de seguretat informàtica del govern dels Estats Units. Aquests es troben a l'abast de tothom qui els vulgui consultar i sovint són utilitzats per empreses o institucions educatives.

La NIST (National Institute of Standards and Technology) ha elaborat una recerca exhaustiva i de manera proactiva per tal de que aquests documents evolucionin i descriguin la manera d'optimitzar els sistemes, les xarxes i les tecnologies d'informació, adaptant els seus continguts a la situació actual.

L'objectiu és que les organitzacions tinguin una guia per tal de planificar i executar tests i proves tècniques de seguretat de la informació, analitzar vulnerabilitats i desenvolupar estratègies per mitigar possibles riscos. També pot ser útil per tal de verificar el compliment d'algunes normatives i marcs legals.

5.3 GDPR

(ICO, 2018) El Reglament General de Protecció de Dades (GDPR, Control (UE) 2016/679) és un reglament europeu per mitjà del qual diferents òrgans oficials busquen reforçar i unificar la protecció de dades per a tots els països de la Unió Europea. Abans de la GDPR, les lleis de protecció de dades venien definides per cada país (com per exemple la LOPD a Espanya, la BDSG a Alemanya o la LIL a França), situació que comportava polítiques desiguals en funció del país, sent en alguns casos massa laxes. També existia una normativa a nivell europeu anomenada Data Protection Directive (Directiva 95/46/EC) de 1995 i a dia d'avui bastant obsoleta.

Amb la GDPR es busca unificar la protecció de dades i aplicar-la a totes les companyies que tractin dades de residents europeus. Aquesta nova llei es va presentar el 27 d'Abril de 2016 i les empreses han tingut al voltant de 2 anys per adaptar-se als requeriments que proposa fins la seva entrada en vigor el 25 de Maig de 2018.

Aquesta llei aplica a dos tipus de dades, sobre les que en fa distinció:

- **Dades personals**

  (ICO, 2018) Qualsevol informació sobre un individu que permeti que aquest sigui directa o indirectament identificat per referencia a la dada en qüestió. Aquesta definició aplica a una gran quantitat de dades entre les que es troben noms, números

de passaport i d'identificació personal de cada país, dades d'ubicació, identificadors online i d'altres.

- **Dades personals sensibles**
  (ICO, 2018) La GDPR tracta les dades personals sensibles com una categoria especial de dades personals. Aquestes categories específiques inclouen dades genètiques i biomètriques, antecedents penals i criminals, dades mèdiques, sexuals, polítiques o sindicals.

Dins dels canvis i incorporacions a aquesta nova llei, es pot destacar la incorporació de la figura del Director de Protecció de Dades o DPO (de l'anglès Data Protection Officer), que serà el màxim responsable de la protecció de dades d'una organització i que serà un càrrec obligatori a organitzacions mitjanes i grans. També s'incorporen restriccions al tractament de les dades per part de les empreses i sancions importants en cas de fuga d'informació.

5.4 PCI DSS

L'Estàndard de Seguretat de Dades per la Indústria de Targetes de Crèdit o PCI DSS (de l'anglès Payment Card Industry Data Security Standard) va ser desenvolupat per un comitè format per les companyies de targetes de dèbit i crèdit més importants com a guia per les organitzacions que processen, emmagatzemen o transfereixen dades de targetes per protegir aquestes dades i evitar el frau sobre aquests actius.

Les organitzacions que processen dades de targetes han de complir amb l'estàndard o s'arrisquen a perdre els seus permisos, a afrontar rigoroses auditories o a pagar importants sancions. A demès, hauran de validar el compliment amb PCI DSS de forma periòdica.

(Margaret Rouse / Tech Target, 2012) La normativa ha anat experimentant canvis i s'han editat noves versions, però principalment especifica els següents requisits:

- Desenvolupament i manteniment d'una xarxa segura.
- Protecció de les dades dels propietaris de targetes.
- Manteniment d'un programa de gestió de vulnerabilitats.
- Implementació de mesures sòlides de control d'accés.
- Manteniment d'una política de seguretat de la informació.

6. Principis de seguretat de l'arquitectura de xarxa

Dins d'aquest capítol es definiran alguns dels conceptes bàsics per entendre les xarxes de comunicacions i que seran necessaris per entendre, més endavant, els conceptes més específics relacionats amb la ciberseguretat. Alguns dels termes explicats en aquest capítol, com per exemple les VLAN o els logs són eines fonamentals per garantir la seguretat d'un entorn.

6.1 Model OSI

El model OSI (en anglès Open Systems Interconnection Model) es un model conceptual que busca estandarditzar les funcions de comunicació d'un sistema, sense tenir en compte la seva estructura interna o la seva tecnologia. El seu objectiu és la interoperabilitat entre diferents sistemes de comunicació que utilitzin protocols estàndard. Tot i que rarament s'implementa sobre xarxes actuals, es considera una referència per estandarditzar el desenvolupament d'aquestes.

El model divideix el sistema de comunicació en capes d'extracció, executant cadascuna d'elles una funció definida i agrupant una sèrie de protocols. Les set capes que especifica el model OSI son les següents:

	Capa	Descripció	Protocols
7	**Aplicació**	És la capa més propera a l'usuari i s'encarrega de mediar entre les aplicacions software i altres capes de serveis de xarxa.	DNS, DHCP, SFTP, HTTPS, IMPA, LDAP, RTP, SSH, SMTP, Telnet
6	**Presentació**	Tradueix dades entre un servei de xarxa i una aplicació, incloent codificació/descodificació de caràcters, compressió de dades i encriptació/desencriptació.	JPEG, MIDI, MPEG, TIFF
5	**Sessió**	S'encarrega de gestionar sessions de comunicació i connexions entre usuaris.	NetBIOS, SQL, ZIP, NFS
4	**Transport**	Gestiona la transmissió fiable de de segments de dades entre diferents punts d'una xarxa, incloent segmentació, reconeixement i multiplexació.	TCP, UDP

3	**Xarxa**	Permet estructurar i gestionar una xarxa amb múltiples nodes, utilitzant adreçament i control del tràfic.	ICMP, IGMP, IPSec, IPv4, IPv6, RIP
2	**Enllaç**	S'encarrega de la transmissió fiable de trames entre dos nodes connectats per una capa física.	ARP, ATM, Frame Relay, MPLS, Token Ring
1	**Física**	Gestiona senyals i s'encarrega de la transmissió i recepció d'unitats individuals (bits) sobre el medi físic.	Bluetooth, Ethernet, Wi-Fi

Taula 2. Capes, definició i protocols del model OSI (Beckhoff, 2014)

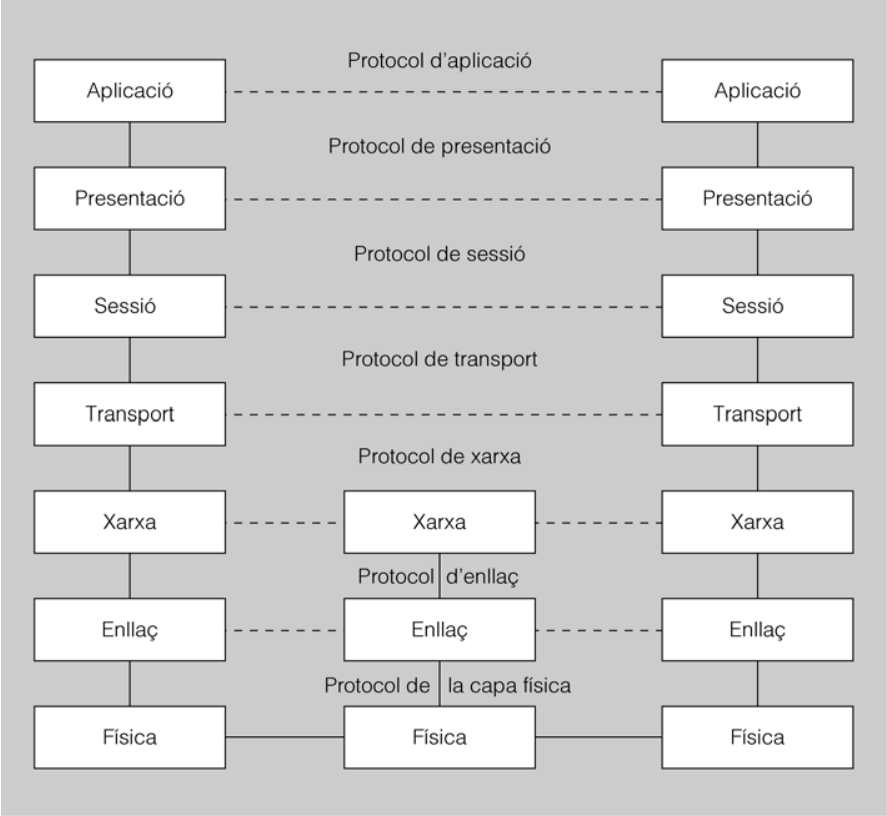

Figura 3 Interacció entre capes del model OSI (IOC, 2013)

Segons aquest model de comunicació, l'emissor (a la esquerra) envia la informació des de la capa d'aplicació cap a les capes inferiors. Aquestes la van encapsulant i hi van afegint una capçalera segons el protocol utilitzat. A la capa de transport s'afegeix s'identifiquen els segments d'informació i s'envien a la capa de xarxa on s'afegeix un altre capçalera. Les dades

es divideixen posteriorment en trames a la capa d'enllaç i s'assigna, de nou, una capçalera a cada trama. A la capa física, la informació pren la forma de bits, que s'entreguen a la xarxa de destí.

Un cop al destí, la informació segueix el camí invers i cada capa va extraient les capçaleres de direccionalment que li pertoquen i envia la informació cap a capes superiors fins que s'entrega el missatge original. Aquest procés s'anomena desencapsulació.

(UPC, 2017) El fet de dividir la comunicació en capes proporciona els avantatges següents:

- Divideix la comunicació en parts més petites i senzilles
- Facilita la normalització dels components de la xarxa amb la qual cosa permet el desenvolupament i el suport de diferents fabricants
- Permet que diferents tipus de maquinari (hardware) i programari (software) es comuniquin entre ells.
- Impedeix que els canvis en una capa afectin a les altres, permetent un desenvolupament més independent.

Tot i que a cadascuna de les capes s'executen les tasques descrites a la seva definició, alguns protocols poden oferir les seves funcionalitats a diverses capes. A nivell de seguretat, totes les capes són responsables d'oferir servei per garantir la confidencialitat, integritat i disponibilitat de la informació, mentre que cadascun dels protocols dins d'una capa ofereixen diferents funcionalitats depenent de la finalitat per la que han estat dissenyats. És per això que alguns prioritzen la seguretat, mentre que d'altres prioritzen el rendiment o d'altres la simplicitat, sempre en funció de l'objectiu principal per al que s'han dissenyat.

6.2 Segmentació de Xarxes

(ISACA, 2016) Mentre que les infraestructures de xarxa continuen evolucionant per satisfer la demanda de nous serveis, millor rendiment i més velocitat, les infraestructures de seguretat no han evolucionat al mateix ritme. Els equips de seguretat es veuen obligats constantment a fer concessions entre el que es permet i el que no, el que es supervisa i el que es controla dels nous serveis de xarxa.

La segmentació de xarxa és el procés d'agrupar lògicament els actius d'una xarxa, els recursos i les aplicacions dins de zones compartimentades que no tenen relacions de confiança entre si i una tècnica comú a l'hora d'implementar seguretat a una xarxa.

D'aquesta manera, cada segment de xarxa pot ser controlat, monitoritzat i protegit de forma independent.

Al introduir la segmentació a una xarxa s'han de tenir en compte alguns requisits clau:

- Obtenir visibilitat del tràfic, dels usuaris i dels actius.
- Protegir les comunicacions i els recursos entre sol·licituds d'entrada i de sortida.
- Implementar controls de tràfic, d'usuaris i d'actius.
- Establir una política de denegació predeterminada a totes les connexions entre segments.

6.3 VLANs

Un element clau en la segmentació són les xarxes virtuals d'àrea local o VLANs (en anglès Virtual Local Area Networks) que són xarxes lògicament independents dins d'una mateixa xarxa física. Els computadors dins d'aquesta xarxa lògica es comporten com si estiguessin connectats al mateix commutador, encara que poden estar en realitat connectats físicament a diferents segments d'una xarxa d'àrea local.

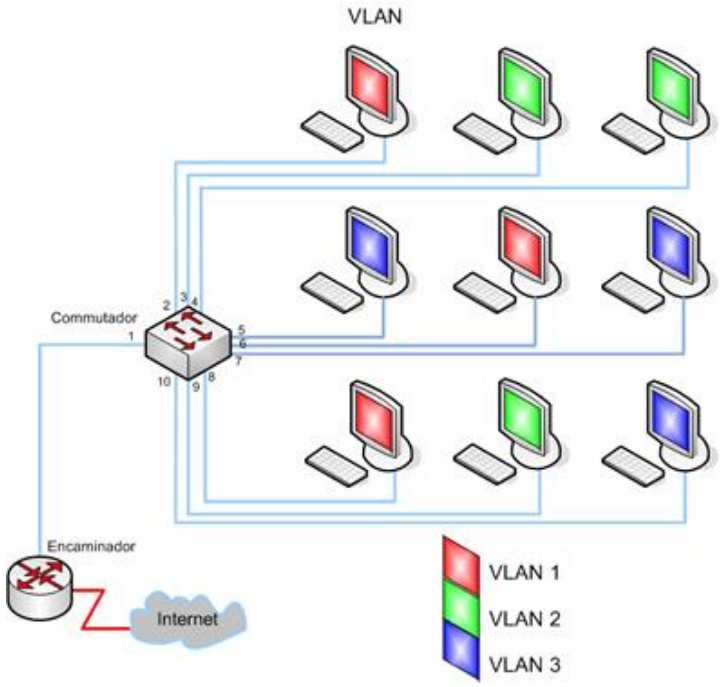

Figura 4 Segmentació de xarxa mitjançant VLANs (IOC, 2013)

Sota el punt de vista de la seguretat, permeten limitar l'accés entre equips ja que per defecte els equips situats a una VLAN no podran veure el tràfic associat a sistemes d'una altra VLAN a la mateixa xarxa física. També permeten als administradors dividir les xarxes per adaptar-les a les necessitats funcionals o de requeriments de seguretat sense haver de fer passar cablejat addicional o fer grans canvis a la seva infraestructura de xarxa.

6.4 Zona desmilitaritzada (DMZ)

(ISACA, 2016) Una zona desmilitaritzada o DMZ (en anglès DeMilitarized Zone) és una subxarxa d'àrea local (LAN) situada entre la xarxa privada (confiable) d'una organització i la xarxa externa (no confiable), normalment Internet.

Amb l'ajuda d'un tallafocs les connexions cap a la xarxa DMZ són permeses tant des de la xarxa exterior com des de la xarxa interna, però no són permeses en canvi, les connexions des de la DMZ cap a la xarxa interna de la organització.

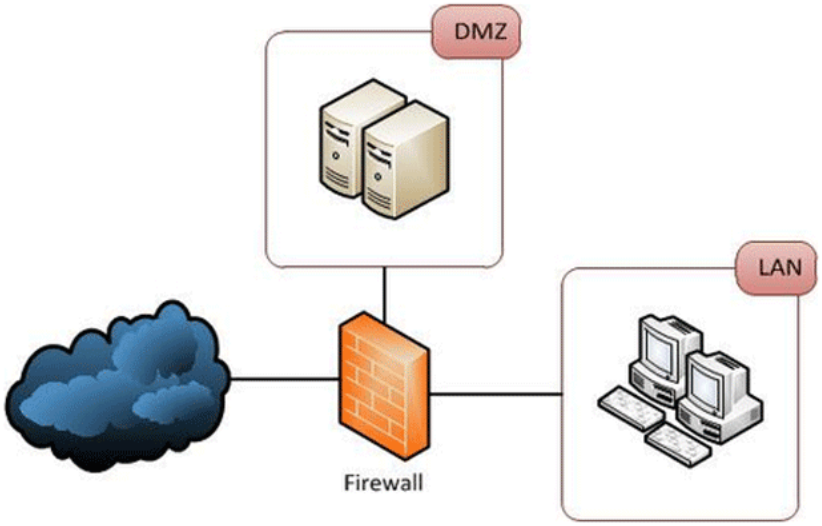

Figura 5. Esquema típic d'una arquitectura amb DMZ (Ymant, 2016)

Els ordinadors/servidors que hi ha en aquesta zona poden allotjar serveis que seran visibles tant des de la xarxa interna com des de la xarxa externa però amb l'avantatge que els ordinadors de la xarxa interna queden aïllats de l'exterior de l'organització, i per tant en cas que algú entrés de forma il·legal des de l'exterior de la xarxa, la única xarxa compromesa seria la DMZ i la xarxa interna quedaria protegida.

És per aquest motiu, que aquest tipus de configuració s'empra habitualment per connectar servidors que allotgin serveis que hagin de ser presentats a l'exterior com per exemple servidors de pàgines web, servidors de correu electrònic, DNS i altres, ja que en el pitjor dels casos únicament aquests ordinadors quedarien compromesos i la resta de dades crítiques quedarien protegides.

6.5 Logs, monitorització i detecció

(ISC2, 2015) Un registre o "log" és un fitxer que conté informació sobre els esdeveniments que afecten a un procés particular dins d'un sistema d'informació. El Logging és el procés d'emmagatzemar informació sobre esdeveniments dins de fitxers log. Aquests fitxers contindran detall sobre el que ha passat, en quin moment, qui ho ha fet i sovint sobre com ha succeït. Per tant, quan s'ha de buscar informació sobre un incident de seguretat, poden donar informació clau i són una de les eines principals per monitoritzar controls i detectar riscos ja que la informació que contenen permetrà alertar sobre violacions de polítiques, comportaments sospitosos, errors o activitats malicioses. D'altra banda, una mala gestió de logs per part d'una organització pot provocar el desconeixement total de qualsevol esdeveniment que comprometi la seguretat així com el retard o la incapacitat d'executar mesures de mitigació o resposta.

Acostumen a existir bastantes dificultats a l'hora de gestionar correctament els fitxers log, com poden ser l'enorme quantitat de fitxers d'aquest tipus que es generen, la dificultat d'extreure'n la informació rellevant, la mala configuració d'aquests o d'altres problemes com pot ser la falta d'espai per emmagatzemar-los o, fins i tot, la despreocupació sobre qui accedeix a aquests fitxers i com hi accedeix. També és important mantenir una correcta segregació de tasques a l'hora de gestionar logs. La capacitat de modificar configuracions d'un sistema mai la pot tenir un individu amb permisos per revisar, modificar o eliminar logs, ja que podria eliminar el rastre d'una acció malintencionada.

(ISC2, 2015) Els logs poden ser de molts tipus, en funció del tipus d'informació que es busqui registrar:

Logs de seguretat Registren informació sobre accessos a recursos com per exemple fitxers, carpetes, impressores o dispositius.

Logs de sistema Guarden informació sobre esdeveniments de sistema, com per exemple quan un sistema s'encén, s'apaga o es reinicia.

Logs d'aplicació Emmagatzemen informació sobre una aplicació específica. En aquest cas, els desenvolupadors de cada aplicació són els responsables d'escollir què és el que volen que aparegui al fitxer log.

Logs de Firewall Els logs de Firewall emmagatzemen informació sobre el tràfic que arriba al dispositiu, incloent tot el tràfic que el Firewall permet i tot el que bloqueja.

Logs de canvi Guarden informació sobre peticions de canvis, sol·licituds, aprovacions i canvis realitzats dins del procediment general de gestió de canvis. Són útils per portar un seguiment dels diferents canvis aprovats a una organització o per tornar a la situació inicial en cas que es detecti que un canvi ha resultat en un incident.

(ISC2, 2015) Els responsables de la monitorització dels logs que es registren a una organització poden recrear esdeveniments que han succeït abans o durant un incident per obtenir informació. És important però, que els atacants no siguin capaços d'accedir als logs ja que en cas de que aquests es puguin modificar de forma malintencionada, podrien esborrar tot registre de la seva activitat, convertint en inútil la informació que contenen. Per això és comú guardar còpies dels fitxers log en una unitat central per tal de protegir-los, per així poder accedir a la informació en cas de que els originals s'hagin modificat o eliminat. Aquestes unitats centrals s'encarreguen de la monitorització d'esdeveniments de seguretat de la informació o SIEM (en anglès Security Information and Event Management) i són un element clau per tal de gestionar de forma automàtica i unificada la monitorització dels sistemes i xarxes d'una organització.

Les organitzacions defineixen sovint polítiques estrictes sobre les còpies de seguretat dels fitxers log. A demés, aquestes polítiques defineixen els anomenats períodes de retenció, que estableixen el temps màxim durant el qual l'organització en qüestió guardarà els logs. Aquests temps poden ser de bastants anys depenent del tipus d'informació i la política interna de l'organització i és comú que vinguin imposats per lleis governamentals o estàndards de seguretat.

7. Principals vectors d'atac

Els vectors d'atac i les metodologies per realitzar-los evolucionen constantment, cosa que representa una amenaça significativa per organitzacions, clients, consumidors i en general per a tothom. Malgrat que alguns atacs s'executen sense cap objectiu concret i el seu objectiu és infectar el major nombre de sistemes sense distingir entre governs, organitzacions o civils, els atacs dirigits es centren en receptors particulars identificats pels atacants sovint després d'una detallada recerca. Accessos no autoritzats a dades o sistemes, instal·lació de programari maliciós, sabotatge d'infraestructures o denegació de servei són alguns dels objectius dels atacants, que cada cop són més creatius i organitzats a l'hora de preparar les seves accions.

Dins d'aquests atacs, en podem destacar tres grups principals:

- Atacs al control d'accessos i identitats
- Atacs a xarxes i comunicacions
- Atacs de codi i aplicacions

És important destacar que algunes de les tècniques utilitzades pels atacants s'utilitzen a més d'un d'aquests grups degut a la seva facilitat de realització o a la seva efectivitat com, per exemple, l'enginyeria social o els atacs d'intercepció d'informació.

És molt important per les empreses conèixer quins són aquests vectors d'atac principals per tal d'anticipar-se i prevenir els seus efectes i també actualitzar-se i mantenir un seguiment de noves formes d'atac per tal de prevenir i adaptar els seus sistemes a aquestes.

Abans de definir aquests tres grans grups d'atacs informàtics, es definiran les amenaces persistents avançades o APTs, que són un tipus d'atac que ha pres una gran rellevància durant els darrers anys a causa de la magnitud dels resultats que es poden obtenir amb ells, fent-los fins i tot aparèixer als mitjans de comunicació a nivell mundial.

7.1 Amenaces persistents avançades

Les amenaces o atacs avançats persistents o APT (Advanced Persistent Threats) són atacs prolongats, de gran complexitat i executats contra un objectiu concret amb la idea de comprometre els seus sistemes i extreure'n informació sensible. Aquests atacs acostumen a ser el resultat de moltes hores de treball d'autèntics equips de criminals informàtics, sovint finançats per grans organitzacions o governs.

(Antoine Vigneron, 2015) Aquest tipus d'atacs presenten moltes fases, no totes elles necessàries depenent de l'objectiu i de la situació, però principalment són les següents:

- **Recollida d'informació** Aquesta fase pot centrar-se en el robatori d'un llistat de treballadors o encara millor, d'antics treballadors disgustats amb l'organització, en conèixer les tecnologies que s'utilitzen dins de l'empresa o en estudiar els accessos dels seus edificis principals.
- **Infiltració inicial** Una eina comú en aquesta fase és l'enginyeria social, amb la qual els atacants poden enganyar als treballadors que anteriorment han identificat per robar les seves credencials o perquè instal·lin software maliciós de manera involuntària.
- **Control i comandament** Un cop s'ha entrat a l'organització l'objectiu serà establir la posició del software maliciós i escampar-lo pels diferents sistemes intentant que no sigui descobert.
- **Escalat de privilegis** L'objectiu d'aquesta fase és intentar aconseguir els màxims privilegis i permisos dins de l'organització per tenir accés a la informació i a les dades que es desitgin.
- **Exfiltració de dades** Un cop s'han obtingut els privilegis necessaris, els atacants recolliran la informació del seu interès i l'enviaran fora del sistema per tenir-ne accés.
- **Manteniment de la posició** Una característica fonamental en aquests tipus d'atacs és que és comú que els atacants mantinguin la seva posició dins de l'organització un cop han finalitzat l'atac, per tal de tenir una porta oberta en cas de que vulguin tornar a robar dades i realitzar algun altre tipus d'atac.

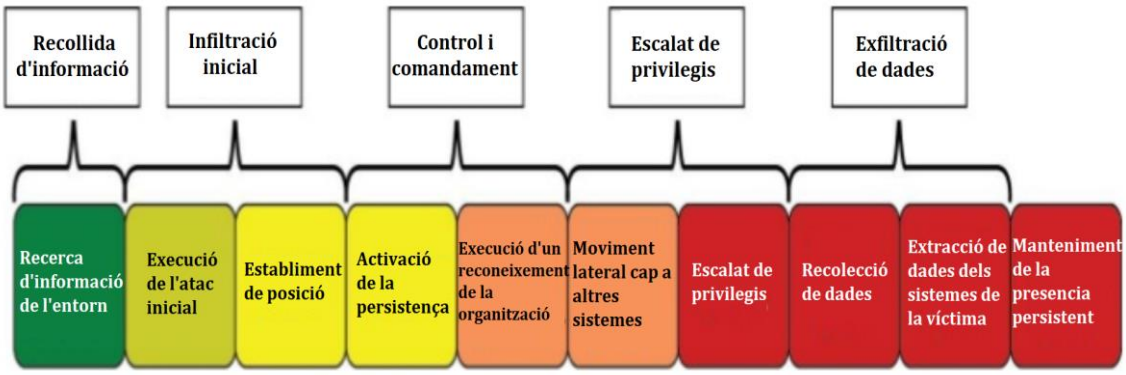

Figura 6. Fases d'un APT (Antoine Vigneron, 2015)

A la imatge superior es poden veure les diferents fases d'un APT, començant per la recollida d'informació sobre el sistema que es vol atacar, passant per la infiltració i l'establiment de

la posició al sistema atacat, fins a l'escalat de privilegis, la recollida de dades i l'extracció d'aquestes del sistema. L'execució complerta d'un atac d'aquest tipus pot durar anys.

En aquest tipus d'atacs, els atacants utilitzen diferents eines i mètodes per deixar la seva empremta i per anar escampant-se pel sistema sense ser detectats, ja que a l'hora de robar informació, una de les parts més importants és mantenir el secret i no ser detectat ja que sovint la informació robada pot perdre ràpidament el seu valor quan l'objectiu s'ha assabentat de l'atac.

(Panda Security, 2017) Segons informes del fabricant de software antivirus Panda, un alt percentatge d'empreses i organitzacions estan sent objectiu d'atacs d'aquest tipus sense que en siguin conscients. El grau de sofisticació del software maliciós que afecta a les xarxes d'aquests grans negocis fa que les eines o capacitats de seguretat habituals no siguin suficients per detectar-los, donant lloc al robatori d'informació confidencial que posteriorment es publica a diversos mitjans i provoca grans pèrdues econòmiques i reputacionals a les empreses.

7.2 Atacs al control d'accessos i identitats

(ISC2, 2015) Aquest tipus d'atacs busquen evitar o traspassar els mecanismes de control d'accés implementats a una organització per tal d'accedir a recursos o tenir permisos que no els hi han sigut autoritzats.

La manera més senzilla d'aconseguir aquest propòsit és tenir les credencials d'usuaris autoritzats i és per això que l'objectiu de molts d'aquests atacs és robar aquesta informació. Un cop els atacants han obtingut les credencials d'un usuari, poden realitzar un atac de suplantació d'identitat, entrant al sistema sota la identitat de l'usuari real, podent accedir als seus recursos i gaudir dels seus permisos. En altres casos, l'atacant pot traspassar directament els mecanismes de control d'accés i accedir directament a les dades.

A continuació es descriuen alguns dels atacs de control d'accessos i identitats més comuns:

7.2.1 Atacs d'agregació d'informació

(ISC2, 2015) Aquest tipus d'atacs utilitzen moltes peces d'informació no sensible que un cop agregades permeten obtenir informació sensible. Un individu o grup recol·lecta moltes peces d'informació sobre un sistema, que un cop juntes s'utilitzen per realitzar un atac.

7.2.2 Atacs de contrasenya

(ISC2, 2015) Les contrasenyes són el mètode d'autenticació més utilitzat i alhora el més dèbil. Si un atacant obté la contrasenya d'un usuari, pot obtenir accés il·limitat a tots els recursos que li han sigut autoritzats. Encara més greu és el cas en el que es robi la contrasenya d'un usuari administrador o privilegiat dins d'un entorn d'alta seguretat, ja que en aquesta situació l'atacant por haver creat altres comptes d'usuari o dreceres per accedir-hi en el futur i la seguretat de l'entorn no es pot tornar a garantir. En aquesta situació, una organització pot arribar a optar per reconstruir el sistema des de zero.

Una contrasenya segura ajuda a prevenir aquest tipus d'atacs. Són comuns les recomanacions i polítiques que demanen una certa complexitat de contrasenya, però també són molts els usuaris que no són conscients de la importància d'utilitzar una contrasenya complexa i de canviar-la de forma regular.

Alguns dels mètodes que utilitzen els atacants per aconseguir contrasenyes són els següents:

- **Atacs de diccionari:** (ISC2, 2015) Intents de descobrir una contrasenya utilitzant totes les possibles combinacions definides dins d'una llista o base de dades de contrasenyes comuns i paraules o caràcters que la gent acostuma a utilitzar.
- **Atacs de força bruta:** (ISC2, 2015) Introducció sistemàtica de totes les possibles combinacions de lletres, números i símbols. Els atacants no acostumen a introduir-les manualment, sinó que tenen programes que proven sistemàticament totes les combinacions.
- **Atacs basats en hashing**: (ISC2, 2015) Les contrasenyes no es guarden en clar a les bases de dades ja que això suposaria una vulnerabilitat evident del sistema, sinó que se'ls hi aplica un hash abans de guardar-les per tal de mantenir-les en secret. Malgrat aquesta mesura, els atacants utilitzen mètodes per intentar esbrinar contrasenyes que generin el mateix hash que es guarda a les bases de dades, com són els atacs *Birthday* i *Rainbow .*

7.2.3 Intercepció d'informació

(ISC2, 2015) Els atacants poden buscar també interceptar el tràfic d'una xarxa amb l'objectiu de trobar credencials d'usuaris (entre moltes d'altres coses) dins dels paquets i unitats d'informació que s'enviïn. Existeixen moltes eines per realitzar aquesta tasca, moltes d'elles fàcilment accessibles. També acostuma a jugar a favor dels atacants el

desconeixement de les persones que, per exemple, es connecten a una xarxa desconeguda a un aeroport o cafeteria o que accedeixen a pàgines web a través de passarel·les.

La facilitat i efectivitat d'aquest tipus d'atacs pot ser disminuïda tenint en compte les següents recomanacions:

- Encriptar totes les dades sensibles (incloent contrasenyes) que s'enviïn a través d'una xarxa.
- Utilitzar contrasenyes d'un sol ús en els casos en que encriptar les dades no sigui possible. En cas de que un atacant intercepti una d'aquestes contrasenyes, no podrà utilitzar-la ja que aquesta només permet accedir al sistema un cop.
- Protegir els dispositius de xarxa amb mecanismes de seguretat física i controlar els accessos per tal de prevenir que els atacants instal·lin programari maliciós que permeti interceptar dades.
- Monitoritzar el tràfic de la xarxa, buscant signatures de programari maliciós. Els sistemes de detecció d'intrusos o IDS (de l'anglès Intrusion Detection System) poden aixecar alertes quan un programa maliciós està interceptant el tràfic d'una xarxa.

7.2.4 Atacs d'emmascarament o suplantació

Aquest tipus d'atacs busquen suplantar la identitat d'alguna cosa, ja sigui una persona física, un sistema, una pàgina web o una direcció de correu. Per exemple els atacants poden utilitzar les credencials d'un usuari autoritzat per accedir a l'edifici que conté la infraestructura IT d'una organització o reemplaçar una direcció vàlida per una falsa per tal d'ocultar una identitat o per fer-se passar per un sistema autoritzat.

7.2.5 Enginyeria social

Sovint, la manera més fàcil d'obtenir informació d'algú és preguntar-li directament i aquest és un dels mètodes més comuns i més efectius que utilitzen els atacants. Els atacs d'enginyeria social busquen guanyar la confiança d'algú utilitzant l'engany, com pot ser l'enviament de correus suplantant identitats, una trucada telefònica o pàgines web fraudulentes. A causa de la popularitat i efectivitat ja comentades, és molt important que l'organització vetlli pel coneixement d'aquestes tècniques per part del personal que hi treballa, ja sigui intern o extern.

(Kaspersky, 2016) Un dels atacs més comuns que utilitza l'enginyeria social és l'anomenat phishing. Aquest tipus d'atacs intenten obtenir informació sensible com per exemple

credencials, dades de targetes de crèdit fent-se passar per una organització legítima o una companyia coneguda. Els atacants acostumen a enviar correus electrònics de phishing de manera massiva i indiscriminada sense saber qui els rebrà però amb l'esperança de que un cert percentatge de receptors respondran. És comú que aquests correus informin a l'usuari d'un problema o situació i posteriorment li demanin que introdueixi les seves credencials per solucionar-lo. D'altres presenten una situació que requereix una resposta ràpida, a vegades informant de situacions rebuscades com el segrest d'un conegut o el cobrament de l'herència d'un familiar llunyà. Aquesta pressió provoca que hi hagi usuaris que caiguin en la trampa i introdueixin les seves dades personals o fins i tot paguin al moment una quantitat econòmica.

Els atacs més sofisticats inclouen enllaços a direccions web falses creades pels atacants que simulen la web real d'organitzacions conegudes, amb l'objectiu de generar confiança a l'usuari i que aquest introdueixi tota la informació possible. De tota manera, sovint és fàcil identificar que una d'aquestes pàgines web és falsa simplement fixant-se en el format, errors ortogràfics, imatges en baixa resolució o males traduccions.

7.2.6 Atacs a targetes intel·ligents

Aquest tipus de targetes ofereixen una autenticació més segura que les contrasenyes, especialment quan es combinen amb un segon factor d'autenticació com pot ser el PIN. Malgrat aquesta millora, aquest dispositius també són sensibles als atacs.

En aquest cas els atacants es centren en analitzar la informació que envia el xip de la targeta cap al lector del sistema que la processi. Així, intenten determinar factors com el consum elèctric del xip o la duració dels processos per determinar informació valuosa sobre l'usuari.

7.3 Atacs a xarxes i comunicacions

Les xarxes i les comunicacions són tant vulnerables als atacs com qualsevol altre aspecte de la infraestructura IT d'una organització, per tant és important conèixer les amenaces a les que aquests sistemes s'exposen per tal de securitzar un entorn, i mitigar tot risc que pugui suposar danys a informació valuosa, recursos i personal. Apart d'això també s'haurà de tenir en compte que els danys també inclouen factors com retards en accedir a informació, denegació d'accés, frau, malbaratament o abús de recursos i pèrdues materials.

Tot seguit s'expliquen alguns dels atacs més comuns sobre xarxes i comunicacions:

7.3.1 Atacs de denegació de servei (DoS i DDoS)

(Paloalto, 2016) Un atac de denegació de servei és un tipus d'atac que es basa en consumir els recursos que ha destinat una organització per a un servei o objectiu concret, per tal de degradar o prevenir l'activitat del sistema. Per imaginar un atac d'aquest tipus en una situació quotidiana, es pot pensar en una multitud de gent que de forma malintencionada entra a una botiga amb l'únic objectiu d'omplir-la per tal de que els clients legítims no puguin entrar o comprar els productes de forma còmoda. Els atacs DoS s'acostumen a realitzar entre un únic atacant i una única víctima i utilitzen algun tipus de sistema intermedi per tal d'ocultar la identitat de l'atacant.

(ISC2, 2015) Hi ha dos tipus principals d'atacs de denegació de servei i en els dos la víctima és incapaç d'executar les seves operacions o serveis habituals:

- Atacs que exploten una vulnerabilitat de hardware o software. L'explotació d'aquestes debilitats o errors intenta produir que els sistemes es pengin, es congelin o que consumeixin tots els seus recursos. El resultat final és que el sistema no pot processar cap tasca legítima.
- Atacs que inunden el canal de comunicacions d'un sistema amb tràfic irrellevant. El resultat també és que el sistema no pot processar tasques legítimes.

(Paloalto 2016) Els criminals que executen aquest tipus d'atacs els dirigeixen sovint a servidors web d'organitzacions d'alt nivell o visibilitat, com poden ser bancs, comerços, plataformes digitals conegudes o institucions governamentals i, poden ser motivats per venjança, xantatge o activisme. Malgrat que els atacs de denegació de servei no acostumen a produir la pèrdua d'informació o actius crítics, poden costar a la víctima molt temps i un gran cost derivat de la indisponiblitat del seu servei i en alguns casos greus danys reputacionals.

(Paloalto, 2018) Una variant dels atacs de denegació de servei o DoS són els atacs distribuïts de denegació de servei o DDoS (de l'anglès Distributed Denial of Service). Aquest tipus d'atacs utilitza un gran nombre de computadores que envien grans volums de tràfic a la víctima per tal de col·lapsar els seus sistemes. Per tal d'aconseguir l'elevat nombre de computadors necessaris per realitzar un atac DDoS, els atacants utilitzen el que s'anomenen botnets o grans xarxes d'ordinadors infectats que participen en l'atac sense ni tan sols saber-ho, dirigint tot el tràfic d'aquestes màquines cap a la víctima i inundant-la.

Com ja s'ha comentat, els atacs DDoS són una variant dels atacs de denegació de servei, però són bastant més populars gràcies a algunes característiques que els diferencien i els fan més forts que els DoS:

- L'atacant pot executar l'atac a través d'una xarxa d'ordinadors infectats sota el seu control, situats tots ells a diferents països. Això els permet ocultar-se darrera d'aquest "exèrcit" d'ordinadors i dificultar el seu rastreig.
- És difícil per part de la víctima identificar quin tràfic correspon a peticions legítimes i quin és el generat pels atacants.
- Són molt difícils de detenir a causa del gran nombre de màquines que han de ser detingudes, al contrari que els atacs DoS on només hi ha una font d'atac.

Malgrat aquestes dificultats, existeixen certes mesures per prevenir aquests atacs i s'han desenvolupat capacitats de seguretat específiques per bloquejar-los.

7.3.2 Redireccionament o enverinament ARP

El protocol ARP s'utilitza per descobrir la direcció MAC (física) d'un sistema utilitzant la seva direcció IP (lògica) associada. Aquest protocol emet sol·licituds a tots els sistemes d'una xarxa demanant qui té associada una determinada IP i el sistema que la tingui respondrà amb la seva direcció MAC.

Aquest procediment bàsic per la comunicació i el funcionament d'una xarxa també és objectiu d'atacs. Els atacants buscaran modificar les sol·licituds ARP per tal d'associar la direcció MAC d'un atacant amb la IP d'un altre ordinador (o de la porta d'enllaç predeterminada) per tal de que el tràfic originalment destinat a aquella IP arribi a l'atacant. Més enllà d'això, els atacants també poden redirigir el tràfic al receptor original un cop l'han analitzat per tal de que no es sospiti de la seva activitat. Aquests atacs poden ser executats des d'un sistema compromès a dins d'una xarxa d'àrea local o des d'una màquina que es connecti directament a la xarxa, cosa que requereix que l'atacant tingui accés directe al segment de xarxa que vol atacar.

La vulnerabilitat principal del protocol ARP que permet aquest atac és la seva falta d'autenticació, la qual permet als atacants enviar missatges ARP modificats a una xarxa d'àrea local. Les mesures que es poden prendre per tal d'evitar atacs d'aquest tipus són utilitzar ARP estàtic per als sistemes més crítics, monitoritzar la memòria cau d'ARP per veure els mapejos que s'han produït o utilitzar sistemes IDS per tal de detectar possibles anomalies.

7.3.3 Redireccionament o enverinament DNS

(Steve Friedl, 2008) Aquest tipus d'atacs també s'anomenen atacs de resolució i el seu objectiu principal és alterar la relació entre el nom de domini i la IP a un sistema DNS per tal de redirigir el tràfic cap a un sistema controlat per l'atacant o per realitzar un atac de denegació de servei.

El mètode més comú que utilitzen els atacants és enviar respostes falses a sol·licituds DNS per intentar que siguin acceptades per sobre de les respostes reals d'un servidor DNS vàlid.

(Steve Friedl, 2008) Una dada destacable en relació a aquest tipus d'atacs és la vulnerabilitat descoberta al 2008 per l'investigador Dan Kaminsky, que permet a un atacant redirigir clients DNS d'una xarxa cap a servidors alternatius de la seva pròpia elecció. D'aquesta manera, enviant respostes falsificades cap a un servidor DNS anunciant subdominis inexistents, un atacant pot apropiar-se dels detalls complerts de resolució d'un domini.

7.4 Atacs de codi i aplicacions

El que s'anomena codi maliciós inclou un ampli ventall d'amenaces a la seguretat informàtica que permeten als atacants explotar moltes vulnerabilitats de xarxa, sistemes operatius, software o seguretat física per tal d'instal·lar programari als sistemes d'una organització. Aquest programari pot presentar diferents propietats per que fa al seu tipus d'acció o el mètode que tenen per propagar-se a través del sistemes en funció de les necessitats que s'hagin tingut en compte a l'hora del seu disseny.

(ISC2, 2015) Una pregunta comú és d'on prové aquest programari. Durant els inicis de la seguretat informàtica, els creadors d'aquest software eren programadors de gran talent que es prenien com un repte o orgull el desenvolupar tècniques innovadores de codi maliciós. Alguns d'ells fins i tot eren útils per tal de detectar errors de seguretat a paquets de software populars, a sistemes operatius o a programari reconegut, aixecant aquestes vulnerabilitats a la comunitat informàtica.

(ISC2, 2015) Actualment, la situació ha canviat i malgrat que segueixen existint els programadors experimentats que s'han comentat, ha aparegut la figura dels anomenat *script kiddies* o individus que no entenen la tecnologia però descarreguen i utilitzen software llest per ser utilitzat per a realitzar atacs contra sistemes remots. Aquesta moda ha donat lloc a una nova tendència en la que qualsevol que tingui uns mínims coneixements tècnics pot descarregar o crear un virus utilitzant eines software dissenyades per aquest propòsit. Aquest conjunt de propietats provoca també que aquests atacs es puguin rastrejar

fàcilment ja que els script kiddies no tenen l'habilitat ni els coneixements necessaris per esborrar-ne les pistes.

A continuació es detallen alguns dels tipus més comuns de programari maligne utilitzat pels cibercriminals, ja siguin experts organitzats o estudiants d'informàtica de primer curs:

7.4.1 Virus

(Alex Haddox, 1997) Un virus informàtic és un tipus de programa maliciós amb les funcions principals de propagar-se i destruir un sistema informàtic. Són la forma més coneguda de programari informàtic i segurament la primera de les formes de codi maliciós que va posar en alerta als administradors de seguretat. Va ser a mitjans del segle XX quan el científic John Von Neumann va presentar un document científic postulant que un programa informàtic es pot reproduir dins d'un sistema. Aquesta teoria es va posar en pràctica donant lloc als primers virus informàtics que han anat evolucionant al llarg dels anys.

(ISC2, 2015) Per definició, els virus han de disposar de tecnologia que els permeti propagar-se de sistema a sistema, aprofitant intercanvis d'informació dels usuaris d'una xarxa. A l'actualitat, els programadors de virus busquen dissenyar-los per incorporar les seves funcions principals (reproduir-se i destruir) de maneres innovadores per tal d'esquivar els sofisticats antivirus actuals. Es podria dir que en els últims anys es viu una autèntica cursa entre els desenvolupadors de virus i els d'antivirus, cadascun d'ells intentant desenvolupar una tecnologia un pas per davant de l'altre.

7.4.2 Cucs

(CISCO, 2017) Els Cucs o Worms en anglès, són un tipus de programari maliciós molt similar als virus però amb una diferència fonamental que els fa més perillosos. Mentre que els virus necessiten l'intercanvi d'un fitxer infectat entre usuaris, els cucs són capaços de replicar-se automàticament a una xarxa sense necessitar la intervenció humana. Per propagar-se, els cucs exploten vulnerabilitats del sistema infectat o utilitzen algun tipus d'enginyeria social per enganyar als usuaris i que els executin.

7.4.3 Troians

(ISC2, 2015) Els administradors de sistemes avisen constantment als usuaris de que mai han de descarregar i instal·lar software d'internet si no estan absolutament segurs de que

prové d'una font fiable. Moltes companyies fins i tot prohibeixen la instal·lació de software que no ha sigut autoritzat i revisat pel departament d'IT. Aquestes polítiques intenten prevenir i minimitzar el risc de que una organització sigui infectada per un troià.

(Kaspersky, 2018) Els troians són un tipus de programari maliciós que es presenta a l'usuari com a software legítim o dins d'un programa aparentment legítim. Els troians es poden utilitzar per obtenir accés als sistemes de l'usuari o organització afectats, els quals són enganyats d'alguna manera per carregar-los i executar-los als seus sistemes. Un cop activats, permeten als cibercriminals espiar, robar dades sensibles o obtenir accessos als sistemes infectats. A diferència dels virus i els cucs, els troians no són capaços de replicar-se per ells mateixos.

(ISC2, 2015) Els troians acostumen a variar molt pel que fa a la seva funcionalitat, alguns busquen destruir tot el que puguin d'un sistema en el menor temps possible, altres segresten el sistema i obliguen a pagar un rescat per desbloquejar-lo mentre que d'altres son bastant inofensius i simplement s'han d'eliminar per alliberar espai i capacitat de processament del sistema.

7.4.4 Ransomware

El ransomware és un tipus de software maliciós que s'ha fet molt conegut sobre tot durant els últims dos anys a causa de la magnitud i la efectivitat dels atacs que ha protagonitzat contra, entre d'altres, grans multinacionals, bancs, empreses de telecomunicacions i plataformes digitals.

(Panda Security, 2017) Aquest tipus de software es transmet com un troià o com un cuc (dins d'un arxiu aparentment legítim) i li dona a l'atacant la possibilitat de bloquejar un dispositiu des de una ubicació remota i encriptar els fitxers del sistema, denegant l'accés a la informació i a les dades emmagatzemades. El software llença una finestra emergent que demana a l'usuari el pagament d'un rescat si vol recuperar el control del seu ordinador, generalment a través d'una moneda virtual per dificultar el seu rastreig.

(Kaspersky, 2016) Segons un informe de l'empresa de solucions de seguretat Kaspersky Lab, l'any 2016 més de 1.445.000 usuaris (incloent empreses) van ser víctimes d'aquests atacs i es van descobrir 62 noves famílies de software d'aquest tipus. Durant els últims anys també s'han fet coneguts grans atacs amb ransomware com WannaCry, NotPetya, CryptoLocker o TeslaCrypt.

Per tal d'evitar aquests atacs es recomana que les organitzacions prenguin les següents mesures:

- No pagar els rescats, ja que encoratgen als atacants mentre que no garanteixen que es recuperi l'accés als fitxers infectats.
- Realitzar còpies de seguretat freqüents per poder restaurar els fitxers en cas que s'infectin.
- No donar informació personal quan es contesti un correu, una trucada o un missatge.
- Utilitzar solucions de seguretat actualitzades.
- Escanejar els correus entrants a l'organització o bloquejar tots els arxius adjunts que puguin suposar una amenaça.

7.4.5 Bombes lògiques

(Stephen Northcut, 2007) Les bombes lògiques són petits programes o seccions de programa que s'activen per mitjà d'un determinat esdeveniment com per exemple una data, una certa capacitat de disc plena, la eliminació d'un fitxer o l'accés d'un usuari. Per exemple un programador pot establir una bomba lògica per esborrar certs fitxers en cas de que deixi l'empresa i el seu usuari es doni de baixa. Al trobar-se originalment dins d'un sistema, aquest tipus d'atac és utilitzat principalment per usuaris interns d'una organització.

(ISC2, 2015) Com la majoria d'objectes de codi maliciós, les bombes lògiques poden prendre diferents formes i mides. Molts virus i troians porten incorporada una bomba lògica per tal de ser activats en el moment en el que l'atacant determini.

7.4.6 Injecció SQL

(Pieter Arntz, 2018) L'SQL o Structured Query Language és un llenguatge de programació dissenyat per manipular i gestionar bases de dades utilitzat a gran part de les bases de dades comercials més comuns (Microsoft SQL Server, Oracle o MySQL, entre d'altres). Els atacs d'injecció SQL es centren en crear o alterar sol·licituds SQL amb l'objectiu de modificar una base de dades de manera malintencionada. La injecció SQL és una amenaça per totes aquelles pàgines o aplicacions web que permeten a l'usuari inserir una sol·licitud SQL a una base de dades sense haver validat la entrada prèviament. Un atacant pot utilitzar aquest tipus d'atac amb l'objectiu de robar informació de la base de dades, entrar-hi informació falsa, prendre'n el control o simplement destruir-la o denegar el seu accés.

(Rapid7, 2018) Els atacs d'injecció SQL es poden produir de diverses maneres, en funció de les vulnerabilitats o els vectors d'atac identificats pels atacants. Un exemple comú d'atac d'aquest tipus es produeix quan un atacant introdueix certs valors que no han sigut validats, com caràcters especials o certs valors que alterin el comportament de la base de dades. Per tal de prevenir aquestes accions, s'acostumen a prendre les següents mesures:

- Evitar posar la entrada d'un usuari directament a una sol·licitud SQL.
- Utilitzar respostes prèviament definides, com llistes desplegables.
- Verificar i validar sempre que el format, caràcters i tipus de dades coincideix amb el que s'espera.
- Xifrar sempre les dades sensibles a una base de dades.
- Limitar els permisos i els privilegis de les bases de dades.
- Evitar mostrar errors de la base de dades directament a l'usuari.
- Utilitzar un tallafocs d'aplicacions web (WAF) per aplicacions que accedeixen a bases de dades.

8. Eines i capacitats de seguretat

Com s'ha vist a l'anterior apartat, la varietat d'atacs i amenaces contra la seguretat de la informació és enorme i no fa més que créixer a mesura que la tecnologia evoluciona. Tot i això, aquesta evolució de la tecnologia també permet que es desenvolupin eines que ajudin a mantenir segura la nostra informació. La varietat d'aquestes també és enorme, tenint grans empreses dedicades a innovar en aquest sentit i en intentar anar un pas per davant dels atacants.

Aquests sistemes de seguretat, amb la seva capacitat de monitorització, permeten tenir a les organitzacions unes eines molt potents per lluitar contra les ciberamenaces. Tot i això, és important recordar que aquestes eines utilitzades de forma aïllada no garanteixen la seguretat d'un entorn per molt potents o innovadores que siguin, sinó que serà la estratègia general, les bones pràctiques definides i la política de seguretat de l'empresa les que determinaran la seguretat de la nostra informació.

A continuació es definiran les principals eines i capacitats de seguretat utilitzades actualment.

8.1 Tallafocs

(CISCO, 2018) Un tallafoc o Firewall en anglès, és un dispositiu de seguretat de xarxa que monitoritza el tràfic que entra i surt d'una xarxa i decideix si permetre o bloquejar cert tràfic en funció de certes regles i polítiques que se li hagin definit. Els firewalls porten sent la primera línia de defensa a la seguretat de xarxa durant més de 25 anys i són l'eina que estableix la barrera entre les xarxes internes confiables i les xarxes externes no confiables com per exemple Internet.

(ISACA, 2016) Un tallafoc consistirà en un sistema o un conjunt de sistemes que reforçaran el perímetre entre dues o més xarxes, formant una barrera entre l'entorn que es considera segur i les xarxes no confiables. Si funciona i es configura correctament, aquest dispositiu haurà de permetre als usuaris de la xarxa interna de l'organització accedir a internet alhora que haurà de prevenir la entrada a la xarxa interna a qualsevol usuari no autoritzat que pretengui entrar (ja sigui des de Internet o des d'una altra xarxa externa no confiable).

La majoria d'organitzacions utilitzen la filosofia de "bloquejar-ho tot" (l'accés a un recurs estarà denegat a menys que es doni una raó de negoci o una necessitat específica per no estar-ho). És important destacar que un tallafocs es pot utilitzar com una eina hardware o

software, presentant cadascuna d'aquestes opcions certs avantatges i inconvenients segons la situació i la utilitat que se'n vulgui donar.

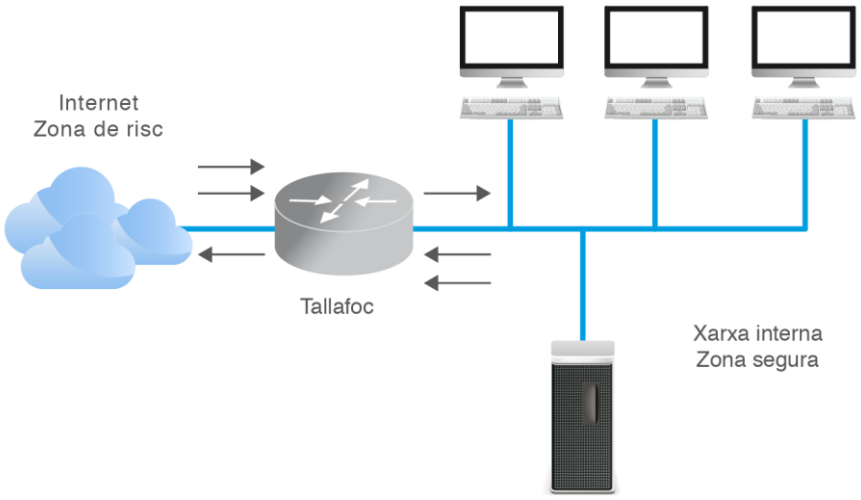

Figura 7. Entrada i sortida de tràfic a través d'un tallafoc (IOC, 2013)

Generalment, els tipus de tallafocs disponibles avui en dia entren dins de les següents categories:

- **Tallafocs de filtrat de paquets** (ISACA 2016) Aquests dispositius treballen a la capa 3 del model OSI, examinant els paquets individuals i acceptant-los o descartant-los en funció de les regles que se li han definit basades en adreces IP, ports o protocols. D'aquesta manera, permeten l'intercanvi directe de paquets entre sistemes externs i interns, cosa que els fa vulnerables a atacs si no estan ben configurats o si les xarxes a protegir són grans.

- **Tallafocs d'aplicació** (ISACA, 2016) A diferència dels de filtrat de paquets, aquests tallafocs permeten que la informació es transmeti entre sistemes però no permeten l'intercanvi directe de paquets. En comptes de confiar en una eina genèrica de filtrat de paquets, s'utilitza un servidor proxy que actua com a intermediari i examina el correcte funcionament d'un determinat servei (per exemple FTP o Telnet) i en fa

modificacions en cas de trobar vulnerabilitats. D'aquesta manera, cap dels sistemes de la xarxa segura pot ser contactat directament per sol·licituds a través d'internet, aportant un nivell de seguretat efectiu.

- **Tallafocs d'inspecció d'estats** (ISACA, 2016) També anomenats tallafocs de filtratge de paquets dinàmic, aquests sistemes porten seguiment de les adreces IP de destí de tots els paquets que surten de la xarxa interna d'una organització. Tan bon punt es rep la resposta a un paquet, es busca la seva referència per veure si el missatge entrant s'ha produït en resposta a una sol·licitud enviada des de l'organització. Aquesta manera de tractar el tràfic permet evitar els atacs que provenen de l'exterior.

- **Tallafocs de nova generació** (ABAST, 2018) Els Next Generation Firewalls (NGFW) són tallafocs que han evolucionat incorporant moltes altres funcionalitats de seguretat com Anti-malware (anti-virus, anti-spyware, anti-spam), IPS (Sistema de Prevenció anti Intrusions), VPN (Xarxa Privada Virtual), entre d'altres. Solucions complertes que a través d'un anàlisi exhaustiu del trànsit de la seva xarxa permeten detectar i minimitzar riscos actius, problemes de seguretat, activitats sospitoses, fuites de dades, etc. Aquest tipus de solucions detecta els riscos ja siguin de procedència interna o externa, quins equips estan compromesos o quins usuaris estan perjudicant la nostra organització fent un ús inadequat de recursos o de la nostra informació.

8.2 Antivirus i Antimalware

Els antivirus són la més coneguda de les eines de seguretat informàtica ja que gairebé tothom en té un instal·lat al seu ordinador de la feina i personal (i si no el té l'hauria d'instal·lar d'immediat). Durant els darrers anys es parla també de les solucions antimalware, que sovint es confonen amb els antivirus i és important veure'n la diferència.

(Malwarebytes, 2017) Com s'ha explicat anteriorment, els virus són peces de codi maliciós que es poden replicar i danyar un sistema informàtic. El Malware, d'altra banda, és un terme genèric que compren una gran varietat de software maliciós com els troians, els cucs, el ransomware i també els virus. Per tant la lògica diria que tots els virus són malware, però el tema és una mica més complex. Els virus es consideren una amenaça heretada, originada fa

ja bastant temps, que porta molts anys en actiu sense haver canviat massa i que actualment no és massa comú, cosa que ha fet que la majoria de fabricants d'antivirus hagin evolucionat per lluitar contra més amenaces que únicament els virus.

(Malwarebytes, 2017) Els antivirus lluiten contra les amenaces més antigues i conegudes com són els Troians, els virus i els cucs. Els antimalware es fixen en amenaces més actuals i complexes, tipus de malware polimòrfic amb gran capacitat de no ser detectat i amenaces "zero day" que son aquelles que encara no han sigut identificades per la comunitat informàtica.

Tot i les seves diferències, aquestes dues eines comparteixen similituds en molts casos pel que fa a la manera que tenen de desfer-se del programari maliciós, utilitzant principalment alguna o un conjunt de les següents tècniques:

Detecció basada en signatures

(Comodo, 2018) És el mètode de detecció més comú en els antivirus tradicionals i es basa en escanejar i revisar els programes, aplicacions i arxius executables d'un sistema per tal de validar si apareixen dins d'un llistat de virus i malware coneguts. També revisa els arxius executables desconeguts buscant errors i comportaments inesperats provocats per la infecció d'un virus.

Per tal de que aquesta tècnica sigui efectiva, aquests llistats de virus i malware han d'estar constantment actualitzats i els proveïdors han de ser capaços de proporcionar aquestes actualitzacions en un món on apareixen milers d'amenaces noves cada dia.

Detecció heurística

(Opswat, 2015) Aquest tipus de tècnica és utilitzada com a complement de la detecció basada en signatures i s'incorpora a la majoria de programes antivirus i antimalware. Es basa en utilitzar regles i algoritmes per tal d'identificar comportaments que puguin indicar que un programa o arxiu és maliciós. El programa antivirus escaneja els arxius del sistema per comparar-los amb la seva base de dades de virus però també té altres solucions d'intel·ligència que li permeten analitzar comportaments, identificar comandes inesperades i recollir informació sobre possibles arxius infectats.

Tot i la millora que aquest sistema aporta sobre la detecció basada en signatures, es requereix un cost computacional més elevat que en primer cas i la probabilitat d'identificar falsos positius és també més elevada.

Detecció per sandboxing

(Oswat, 2015) Una alternativa molt utilitzada a les dues tècniques anteriorment descrites i que també les pot complementar, és el sandboxing. Aquest mètode consisteix en el desplegament d'un entorn controlat (en alguns casos virtualitzat i en d'altres físic) on s'executen els arxius potencialment maliciosos per tal d'analitzar el seu comportament i veure, en cas de que l'arxiu sigui efectivament maliciós, què és el que fa i com actua. Al ser un entorn controlat, els efectes del virus no tenen cap repercussió a sistemes que estiguin fora de l'entorn i l'amenaça es pot estudiar amb més detall.

Una gran avantatge del sandboxing és el fet de que l'arxiu s'obre i s'executa realment, cosa que permet veure de forma exacta el comportament del virus o malware. També és comú que les eines de sandboxing no només indiquin si l'arxiu és maliciós o no, sinó que també generen un informe amb un gran nivell de detall del comportament estudiat, el qual pot ser de gran utilitat com a resposta a un incident per tal d'identificar les intencions dels atacants.

També els entorns de sandboxing acostumen a ser altament personalitzables, oferint la possibilitat de crear entorns "a mida" on es poden executar arxius sobre determinades màquines o fins i tot replicar els virus per obtenir un anàlisi més complert.

Tot i la seva flexibilitat, aquesta tècnica també té limitacions. És comú que els programadors de malware introdueixin mecanismes per evitar que el seu software es reprodueixi en aquest tipus d'entorn. Aquestes tècniques poden ser des de impedir que el programa s'executi sobre màquines virtuals o d'altres mètodes més sofisticats per distingir si s'està executant sobre un entorn de sandbox o no.

Tots tres mètodes presenten fortaleses i debilitats úniques que són útils en diverses situacions. El màxim grau de seguretat que pot aportar un sistema antivirus o antimalware vindrà donat per la utilització de tots tres mètodes de forma simultània, passant per

diverses capes d'escaneig, per tal de minimitzar el nombre de mostres que puguin evadir la detecció.

8.3 SIEM

(SANS Institute, 2006) És comú que els acrònims anglesos SEM, SIM i SIEM s'utilitzin de manera intercanviable. L'àrea de la seguretat que s'encarrega de la monitorització en temps real, la correlació d'esdeveniments, i els informes i notificacions s'anomena gestió d'esdeveniments de seguretat o SEM (de l'anglès Security Event Management). La segona àrea proporciona emmagatzematge, anàlisi, gestió i presentació de dades generades a partir dels logs generats pels sistemes en un període més ampli i s'anomena gestió d'informació de seguretat o SIM (Security Information Management). Degut a la evolució d'aquestes tecnologies, que cada cop incorporen més capacitats, es parla de solucions SIEM (Security Information and Event Management), les quals són eines que permeten recollir, analitzar i presentar informació sobre sistemes, xarxes, dispositius o aplicacions. Tot i que com es veurà posteriorment, els sistemes SIEM cada cop incorporen més funcionalitats, aquestes eines tenen tres funcions fonamentals:

- Recollir i emmagatzemar els logs generats pel sistema de forma centralitzada.
- Analitzar els logs per identificar accions malicioses.
- Generar informes i presentar informació obtinguda.

(Deloitte, 2017) Un dels principals motius que porten a les organitzacions a invertir en un sistema SIEM és la possibilitat de centralitzar els esdeveniments de seguretat sobre una única plataforma. Dins d'una organització d'un volum considerable, es generen milers de logs per segon, que provenen de servidors, dispositius, sensors, aplicacions, eines i d'altres sistemes. És molt còmode disposar d'una eina que permeti centralitzar-los i analitzar-los des d'una única plataforma en comptes d'anar sempre a buscar-los al sistema que els ha generat. També suposa una gran avantatge pel que fa a la gestió d'incidents, ja que la centralització de logs sobre una única plataforma evita que l'administrador d'una màquina local pugui modificar-los o esborrar-los per ocultar possibles accions malicioses.

És important també tenir en compte que no tots els logs generats es podran enviar al SIEM, ja que no tota la informació que es genera a la xarxa és rellevant com per ser analitzada. També s'ha de tenir en compte que la capacitat d'aquesta i de qualsevol altra eina és limitada pel que fa al volum de dades que pot emmagatzemar i processar, per tant és molt important valorar quins logs són realment importants com per ser integrats al SIEM i quins no.

(Deloitte, 2017) La majoria de sistemes SIEM utilitzen un agent que es desplega sobre els sistemes dels que es volen recollir els logs i que envia aquests a una consola d'administració centralitzada on aquests són analitzats en temps real per tal d'identificar comportaments anòmals a la xarxa. És aquí on comença l'anàlisi o correlació de logs, entesa com la relació entre dos o més esdeveniments generats en el mateix o en diferents dispositius dins d'un cert període temporal i que s'utilitza per detectar una acció. Aquest anàlisi suposa la part fonamental del funcionament del SIEM, ja que si l'eina no es configura per tenir aquesta intel·ligència, es converteix simplement en una base de dades amb centenars de milers de logs dels que no es podria treure cap informació.

Un cop s'analitzen les accions, es generen alertes per avisar als equips de seguretat sobre possibles accions malicioses. Per exemple, si un usuari inicia sessió al seu compte de correu des de Barcelona i en només 2 hores la inicia des de Filipines, el SIEM haurà de ser capaç d'extreure aquesta informació dels logs generats pel sistema i d'alertar que s'està produint una situació anòmala per tal de que els equips de seguretat prenguin mesures segons les polítiques definides. També és possible configurar regles més complexes, que utilitzin la informació de diferents esdeveniments que provinguin de diferents fonts, com per exemple podria ser una regla que relacioni els esdeveniments d'un Proxy que indica que un usuari s'ha connectat a un domini sospitós i els esdeveniments de l'antivirus que indiqui la presencia de programari maliciós al dispositiu de l'usuari.

Finalment, el SIEM permet presentar tota aquesta informació de manera clara, facilitant la feina als equips de seguretat, els quals podran treure informes, generar gràfiques i identificar fàcilment l'estat de la xarxa i els comportaments dels sistemes i usuaris.

(Deloitte 2017) Al estudiar els sistemes SIEM actuals, ens trobem amb un mercat de fabricants molt ampli on cadascun hi afegeix i presenta diferents funcionalitats, des de les bàsiques anteriorment descrites fins a d'altres més sofisticades, d'entre les que podem destacar les següents:

- Detecció d'anomalies i irregularitats a la xarxa.
- Anàlisi del comportament d'usuaris.
- Anàlisi i topologia de xarxes.
- Configuració de dispositius.
- Priorització de vulnerabilitats.
- Anàlisi d'errors i simulacions.
- Gestió d'incidents i alertes de seguretat.

Tot i les enormes avantatges que presenta un SIEM per una organització, aquestes tecnologies són cares, complexes d'administrar i requereixen personal qualificat que les configuri i les mantingui. És per això que són més comuns en grans organitzacions, mentre que les mitjanes empreses acostumen a optar per altres tipus de solucions de monitorització no tant potents però amb un cost inferior.

(UPC, 2017) Els costos poden variar àmpliament depenent dels factors principals com les capacitats del SIEM, el fabricant, el volum d'informació a processar, la mida de la xarxa i la seva topologia. Principalment, s'ha de tenir en compte l'impacte que causa aquest al sistema, ja que al ser una eina amb capacitats d'anàlisi en temps real, requereix un hardware adequat, amb uns recursos dedicats que permetin obtenir el rendiment desitjat.

Aquest factor és primordial per decidir si una organització és capaç de gestionar el seu SIEM desplegat on-premise o bé haurà de recórrer a altres solucions com el lloguer de servidors online o contractar un SIEM desplegat al núvol.

(UPC, 2017) Desplegar la solució on-premise requerirà dedicar uns recursos d'emmagatzematge, CPU i RAM al servei, a més de la configuració d'aquest, que acostuma a ser complexa. Per altre costat, contractar un SIEM implementat al núvol no requerirà d'una configuració inicial, ni d'una gestió, ja que se n'encarreguen els que ofereixen el servei, però aquesta solució acostuma a ser més cara.

Un cop desplegat el SIEM, s'haurà de configurar per adaptar-lo a les necessitats de la nostra organització, i gestionar-lo de la mateixa manera. És un procés més complex que contractar un SIEM al núvol, però d'aquest mode ens assegura que les dades no surten del nostre entorn, i que el personal que tracta les dades que poden ser crítiques, és personal de la mateixa organització.

8.4 DLP

(Symantec, 2015) Un dels principals maldecaps pels administradors de seguretat és la fuga d'informació. Són milers els documents que es comparteixen durant el dia a dia d'una organització, correu electrònic, dispositius d'emmagatzemament extraïble, pujada de documents a pàgines web, descàrrega de documents a unitats locals, etc. Aquesta enorme quantitat d'informació juntament amb la també gran quantitat de canals de comunicació provoquen que sigui molt difícil controlar quanta i quina informació es filtra a l'exterior.

Segons un estudi de Symantec, el 64% de la fuga d'informació és provocada per usuaris ben intencionats, que descarreguen o envien informació confidencial involuntàriament. El mateix estudi indica també que el 50% dels treballadors es queden amb dades confidencials quan deixen la seva empresa. L'estudi de Symantec conclou que, considerant tant els incidents intencionats com els involuntaris, a l'any 2012 es van produir als Estats Units al voltant de 2100 incidents, provocant pèrdues estimades en 3.5 milions de dòlars a empreses i administracions. A demés, sovint hi ha una conseqüència encara més greu que els costos econòmics, i és el fet de posar la nostra organització en el punt de mira, amb el cost reputacional que això suposa.

La entrada en vigència de la GDPR aquest any és també un motiu de pes per que les organitzacions utilitzin solucions per evitar la filtració de les seves dades i les dures multes que aquesta nova regulació planteja.

(Kaspersky, 2017) El primer pas per protegir la informació d'una organització és tenir clar i classificar quina informació, dins del gran nombre de fitxers que emmagatzema l'organització, és realment confidencial i quina no. Principalment, es voldrà protegir les dades personals de clients i treballadors, les dades de targetes de crèdit, registres mèdics, números de la seguretat social, informació sobre estats financers, informació amb propietat intel·lectual, documents d'estratègia de negoci, documents de recursos humans i d'altres dades que es considerin sensibles depenent de la tipologia de l'empresa.

(Symantec, 2015) Un cop sabem quines dades s'han de protegir el següent pas és saber on s'emmagatzemen aquestes dades i qui les utilitza i en té accés. Existeixen eines de prevenció de fuga o pèrdua de dades (DLP de l'anglès Data Loss Prevention) que permeten identificar les dades confidencials de l'organització, monitoritzar el seu ús i en cas necessari prevenir la fuga d'aquesta informació.

(Symantec, 2015) Les eines disponibles al mercat per realitzar aquesta tasca són molt diverses i les seves funcionalitats i característiques varien molt en funció del fabricant. A nivell general, es tractarà de sistemes que s'encarregaran d'analitzar el tràfic de la xarxa i analitzar si el que s'està enviant a l'exterior és documentació confidencial, per en aquest cas, bloquejar-lo o informar sobre l'incident. Aquesta identificació es porta a terme principalment indexant el conjunt de documents que es vol protegir (d'una manera semblant a la detecció per signatures que s'ha comentat anteriorment), afegint una paraula clau als documents o configurant regles al DLP que detectin informació confidencial, com per exemple, reportar una alerta en cas que es detecti l'enviament d'un document que

contingui vuit números seguits d'una lletra (cosa que indicaria la fuga d'informació d'un número de DNI).

De la mateixa manera que per altres capacitats de seguretat, pel DLP també és molt important la seva ubicació dins de la xarxa de l'empresa. Situar aquests sistemes als punts de sortida a Internet de l'organització donarà una gran visibilitat ja que es detectarà tot el tràfic que surt d'aquesta. També és comú instal·lar un agent de DLP als dispositius finals dels usuaris per tenir major control sobre la informació que s'emmagatzema i per identificar si per exemple es descarreguen dades sensibles a unitats locals fora de la xarxa de l'organització.

8.5 IDS/IPS

(Juniper, 2018) Una típica xarxa empresarial està constituïda per multitud de punts d'accés cap a altres xarxes, tant públiques com privades. El repte principal al que les organitzacions s'exposen és mantenir la seguretat envers aquestes xarxes mentre es mantenen obertes i accessibles a treballadors i clients.

(ISC2, 2015) Dos elements molt utilitzats i encarregats de mantenir la seguretat a les xarxes són els sistemes de detecció d'intrusions o IDS (de l'anglès Intrusion Detection System) i els sistemes de prevenció d'intrusions o IPS (de l'anglès Intrusion Prevention System). Aquestes eines complementen al tallafocs a l'hora de protegir la xarxa i s'encarreguen de monitoritzar les anomalies que s'hi produeixen.

(Juniper, 2018) La detecció d'intrusions és el procés de monitorització d'esdeveniments que succeeixen a una xarxa i l'anàlisi d'aquests per identificar incidents o amenaces. La prevenció d'intrusions és el procés de realitzar una detecció d'intrusos i aturar l'acció dels possibles incidents.

(Devin Morrisey, 2018) Els sistemes IDS i IPS treballen analitzant de forma ininterrompuda la xarxa sobre la que s'han desplegat, identificant possibles incidents i generant logs sobre ells, aturant els incidents i reportant-los als equips de seguretat. Aquests sistemes s'han convertit en una adquisició necessària per als equips de seguretat de la majoria d'organitzacions precisament perquè són capaços d'aturar als atacants mentre recullen informació de la xarxa.

(Devin Morrisey, 2018) Al parlar de les diferències entre un IDS i un IPS, podríem dir que són similars en molts aspectes, però es diferencien en que l'IPS és capaç de, un cop detectat

el tràfic no desitjat, prendre accions i aturar-lo. Aquesta característica afegida als IPS ha de ser controlada i configurada correctament per tal d'evitar que el sistema bloquegi també el tràfic legítim, a causa de la identificació de falsos positius.

Sabem doncs, que els IDS i IPS detecten anomalies, però és més difícil explicar de quin tipus d'anomalies es tracta perquè dependrà de molts factors, del tipus de xarxa i de la configuració del sistema. Principalment, es podria dir que aquests sistemes es centren en identificar tràfic inusual, tràfic que no volem a la nostra xarxa, tràfic prohibit o alguns tipus de malware.

(Juniper, 2018) Aquests sistemes acostumen a treballar de tres maneres:

- **Detecció basada en signatures**
  De manera semblant a com passa amb els antivirus i antimalware, els IDS i IPS també utilitzen bases de dades de signatures per comparar-les amb el tràfic real i identificar possibles incidents. Aquest és el mètode de detecció més simple ja que simplement compara paquets o logs que circulen per la xarxa amb les signatures que té guardades.

- **Detecció basada en anomalies**
  Aquest mètode compara definicions del que es considera "activitat normal" a una xarxa amb el comportament real que s'està produint per tal d'identificar desviacions. Aquest mètode pot ser molt comú per detectar amenaces no conegudes prèviament.

- **Anàlisi d'estats de protocols**
  Aquesta tècnica va un pas més enllà i compara els comportaments acceptats i benignes per a cadascun dels estats dels protocols utilitzats per intentar identificar desviacions.

(Devin Morrisey, 2018) Una de les claus del correcte funcionament d'aquests sistemes és ubicar-lo de forma correcta, i no parlem de la seva posició dins del rack al nostre CPD, sinó el segment de xarxa que estarà monitoritzant. Per exemple, seria inútil inspeccionar el tràfic que arriba a la part pública del tallafoc ja que les polítiques d'aquest ja s'encarreguen de filtrar el tràfic no desitjat. Una opció és situar l'IDS o IPS per tal de monitoritzar un switch intern (com per exemple a una LAN o a una DMZ) cosa que permetria analitzar el tràfic a determinats servidors clau però es perdria la visibilitat sobre altres parts de la xarxa.

8.6 VPN

(CISCO, 2008) El món empresarial ha canviat molt durant les últimes dècades. Més enllà de gestionar entorns a nivell regional, molts negocis actuals han de pensar en mercats globals i la logística que comporta accedir-hi. Les grans organitzacions tenen instal·lacions distribuïdes entre diferents països a tot el món. Això provoca una necessitat bàsica per a totes elles: poder mantenir comunicacions segures, ràpides i fiables siguin on siguin les seves oficines.

Fins fa relativament poc, aquest tipus de comunicacions confiables només era possible per mitjà de línies dedicades per establir una WAN sobre una gran àrea geogràfica. Aquesta solució comporta grans avantatges sobre una xarxa pública a nivell de rendiment, seguretat i fiabilitat, però també comporta uns costos molt elevats, sovint impossibles d'assumir si es tracta de grans distàncies. Les línies dedicades tampoc són viables en els casos en que la major part dels usuaris i treballadors executen les seves funcions en un entorn mòbil i necessiten accedir freqüentment a la xarxa privada de la seva organització.

A mesura que la popularitat d'Internet a anat creixent, els negocis han trobat maneres d'expandir les seves pròpies xarxes. Primer van ser les Intranets, utilitzades únicament per treballadors de l'organització, mentre que uns anys enrere es van començar a utilitzar les xarxes privades virtuals o VPN per suportar les necessitats dels treballadors en remot i les oficines a distància.

(CISCO, 2008) La xarxa privada virtual o VPN (de l'anglès Virtual Private Network) és una tècnica de virtualització que s'utilitza per crear una xarxa privada entre diferents nodes sobre la infraestructura d'una xarxa pública com por ser Internet. D'una manera més concreta, es podria dir que una VPN permet a dues o més xarxes que utilitzin un rang privat d'IPs, comunicar-se sobre internet com si únicament estiguessin separades per un router local, utilitzant connexions virtualitzades en comptes de connexions reals dedicades.

(HKSAR, 2008) Les VPN transmeten les dades a través d'un túnel virtual. Abans d'enviar un paquet, aquest s'encapsula en un nou paquet amb una capçalera diferent que contindrà informació que permeti encaminar-lo cap al seu destí sobre una xarxa pública. El camí lògic que seguirà aquest paquet és el que s'anomena túnel virtual, però és important entendre que únicament amb aquest túnel no es proporciona seguretat a les dades. Per proporcionar confidencialitat a la informació enviada, les VPN utilitzen també xifrat sobre les dades abans d'encapsular-les dins del túnel virtual, garantint que no es podrà accedir ni modificar cap

dels paquets que es transmetin sobre la xarxa pública. Aquest és probablement el servei més important que proporciona un proveïdor de VPN. Els protocols més comuns per portar a terme aquesta acció són IPsec, L2TP, PPTP i SSL (tots treballant entre les capes dos i tres del model OSI) i alguns d'ells proporcionen també funcionalitats addicionals com control d'integritat de dades, autenticació d'origen i identificació d'errors.

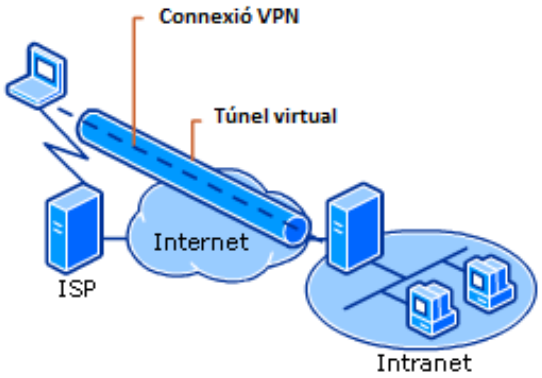

Figura 8. Exemple d'implementació d'una VPN (Microsoft, 2014)

(CISCO, 2008) Existeixen dos tipus principals de VPN:

- **VPN d'Accés Remot**

  També anomenades VPDN (Virtual Private Dial-up Network), constitueixen connexions entre un usuari i una xarxa d'àrea local i són utilitzades per organitzacions que necessiten que els seus treballadors es connectin de forma remota des de diferents ubicacions. Típicament, les organitzacions proporcionen algun tipus de compte als usuaris que els permeti identificar-se i utilitzar el seu client VPN per connectar-se de manera segura i xifrada a la xarxa privada de l'organització a través d'un proveïdor de servei d'internet (ISP).

- **Xarxa Site-to-Site**

  Per mitjà de la utilització d'equipament dedicat i de tècniques de xifrat a gran escala, una organització pot connectar múltiples ubicacions fixes sobre una xarxa pública compartida, com per exemple Internet. Cadascuna d'aquestes ubicacions únicament necessita una connexió a aquesta xarxa pública, suposant un estalvi molt important en línies privades dedicades. Quan aquest tipus de connexions es produeixen entre oficines o ubicacions de la mateixa organització, es parla sovint d'Intranet VPN,

mentre que quan s'utilitzen per connectar l'organització amb un client o proveïdor, s'anomenen Extranet VPN.

Així doncs, una xarxa virtual privada correctament dissenyada permetrà ampliar la connectivitat geogràfica d'una organització, reduir els costos respecte a una WAN tradicional, simplificar la topologia de xarxa i reduir els costos pel que fa a usuaris o treballadors, al mateix temps que s'incrementa la seva productivitat.

8.7 PAM

En un entorn IT es consideren usuaris privilegiats tots aquells que tenen accessos d'administració a sistemes crítics. Per exemple, són els usuaris que poden crear i eliminar comptes en un servidor de correu i que poden realitzar canvis de configuració en màquines i servidors. Com qualsevol altre privilegi, només es pot concedir a certs tècnics i administradors de sistemes de confiança, però tot i això, des del punt de vista de la seguretat, no es pot atorgar mai aquesta confiança sense que la seva operació estigui controlada i monitoritzada.

Aquests usuaris requereixen una gestió especial ja que en cas de que es comprometin les seves credencials o es produeixi el robatori d'alguna d'aquestes identitats per part d'un atacant, aquest tindria accés directe a aquests sistemes crítics per poder canviar configuracions, desconnectar sistemes, esborrar dades i comptes d'usuari o instal·lar programari maliciós, suposant tot això un impacte altíssim per l'organització.

(Wallix, 2016) Per gestionar aquest tipus d'usuaris, s'han desenvolupat les eines PAM o Privileged Access Management, que s'encarreguen de mantenir a l'organització segura davant el mal ús, intencionat o no intencionat dels usuaris privilegiats. Aquestes eines són especialment necessàries a mesura que augmenta la mida de l'organització i de la seva infraestructura IT, ja que això suposarà la existència de més usuaris privilegiats. Moltes organitzacions fins i tot han reportat que tenen tres cops més usuaris privilegiats que usuaris normals.

Una solució PAM ofereix una manera segura i pautada d'autenticació per aquest tipus d'usuaris i una monitorització explícita de les accions realitzades sobre tots els sistemes rellevants. Les característiques principals d'aquestes eines son:

- Proporcionar privilegis als usuaris única i exclusivament sobre els sistemes per als que estan autoritzats.
- Proporcionar accés única i exclusivament durant el temps que es necessita i revocar-lo un cop la necessitat expiri.
- Evitar la necessitat de que els usuaris privilegiats utilitzin contrasenyes locals i directes.
- Gestionar l'accés sobre sistemes heterogenis d'una manera centralitzada.
- Generar informes d'auditoria inalterables per a totes les operacions que facin ús de privilegis.

(Cyberark, 2018) Les solucions PAM varien en la seva arquitectura en funció del fabricant, però principalment ofereixen els següents components o mòduls:

- **Gestor d'accessos**

  Aquest mòdul governa l'accés sobre les comptes privilegiades, actua com a únic punt de definició de polítiques i força als usuaris privilegiats a complir amb aquestes polítiques per accedir als sistemes. El gestor d'accessos coneix a quins sistemes té accés cada usuari i a quins no i el seu nivell de privilegi (si pot realitzar canvis, quins tipus de canvis pot realitzar, durant quin període, etc). Sobre aquest component apareix també la figura del Super Administrador, que és qui té permís per afegir, modificar o eliminar usuaris administradors. El seu paper és clau per tal de concedir permisos als usuaris i per reduir el risc de que antics treballadors d'una organització conservin permisos privilegiats, situació que és bastant més comú a les empreses actuals del que es podria imaginar.

- **Gestor de contrasenyes**

  Una característica fonamental dels sistemes PAM és que en cap moment proporcionen la contrasenya real d'administració dels sistemes crítics als usuaris privilegiats. En comptes d'això, l'eina emmagatzema la contrasenya de forma segura i obre l'accés als sistemes un cop l'usuari privilegiat s'ha autenticat. Això evita el risc de que un usuari pugui accedir de manera directa a un dispositiu físic coneixent la seva contrasenya d'administració.

- **Gestor de sessions**

  Malauradament el control d'accessos no és suficient, ja que es necessita saber quines accions han realitzat els usuaris, sobre quins sistemes, a quina hora i quines

conseqüències han tingut. Aquest mòdul s'encarrega de registrar totes les accions realitzades per un usuari administrador durant la seva sessió.

9. Cas pràctic

9.1 Introducció

[Gartner, 2018] Cada cop més organitzacions decideixen confiar en els serveis cloud per suportar els seus recursos IT i la seva gestió i processament de dades, cosa que ha provocat un enorme augment en la demanda d'aquests serveis i que seguirà creixent durant els propers anys. La consultora Gartner preveu que a l'any 2020 el 92% del processament de dades a nivell mundial s'executarà en cloud.

Tot i aquesta tendència, també es comú que les organitzacions tinguin dubtes a l'hora de confiar en el cloud per a la realització de determinats serveis o per emmagatzemar certes dades ja que creuen que aquests procediments es realitzaran de forma més segura i controlada si s'executen dins de la pròpia organització enlloc de confiar aquesta responsabilitat a un tercer.

L'objectiu d'aquesta part del treball és realitzar una comparativa entre la securització d'un servei de correu i d'emmagatzemament d'informació on-premise i d'un servei cloud. S'analitzaran les característiques entre els dos paradigmes per tal d'identificar les seves diferències principals i veure com afecten aquestes a la seguretat.

9.2 El correu electrònic corporatiu

[Dell, 2017] El correu electrònic és un dels serveis crítics per a una organització, necessari per la comunicació entre treballadors, el contacte amb clients i proveïdors, l'intercanvi d'arxius i també per la gestió de tasques, contactes, calendaris i reunions. Alhora, és un dels serveis que més ha experimentat la migració cap al cloud durant els darrers anys. En un estudi realitzat per Dell sobre els entorns de correu dels professionals IT, un 44% dels participants afirma que la seva organització utilitza una solució de correu exclusivament on-premise, mentre que un 42% utilitza un model híbrid entre on-premise i cloud. Dels participants a l'estudi que utilitzen la solució exclusivament on-premise, aproximadament un 50% tenen previst mantenir el servei de la mateixa manera durant els propers anys, per un 43% que afirmen estar avaluant opcions al cloud.

A continuació també es mostren alguns dels resultats d'aquest estudi, realitzat sobre organitzacions amb més d'un miler d'usuaris:

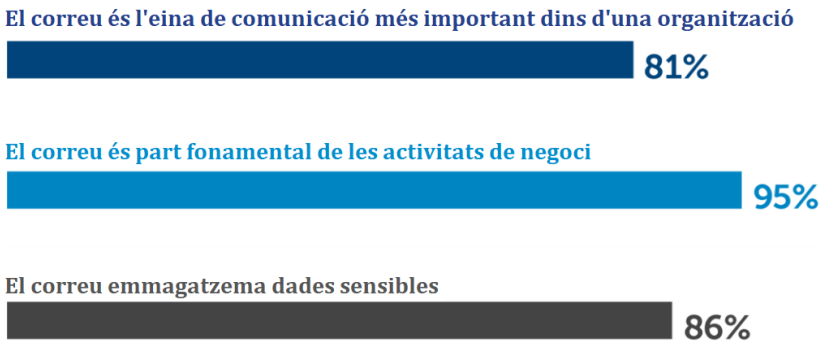

Figura 9. Estudi de Dell sobre el correu corporatiu (Dell, 2017)

Aquests resultats posen de manifest la necessitat de desenvolupar una solució de correu que tingui en compte la usabilitat necessària per aquest servei i les preocupacions dels membres de l'organització sobre les seves dades independentment de que l'entorn on es treballi sigui on-premise o cloud.

Durant els últims anys s'han vist principalment tres models de desenvolupament i prestació de correu corporatiu, que coincideixen amb els tres models típics per a la resta de serveis com són les solucions **on-premise** al propi Data Centre de l'organització, en **cloud** a través d'un proveïdor extern o un model **híbrid** que combina els dos paradigmes per tenir part del servei on-premise i part del servei en cloud.

Pel correu corporatiu, una de les solucions més adoptades ha sigut Microsoft Exchange, que en els últims anys s'ha vist substituïda per la seva versió cloud amb Office 365, també de Microsoft.

9.3 Entorn on-premise a securitzar

L'entorn a securitzar serà tot el que inclou des de l'accés d'usuari al correu, passant per una solució d'emmagatzemament d'informació on els usuaris podran guardar els seus documents, fins a la sortida a internet del correu.

Es considerarà que tots els recursos per proporcionar aquest servei a l'usuari es troben a un Centre de Processament de Dades (CPD) controlat exclusivament de manera interna per l'organització, qui serà la responsable de la correcta utilització de les instal·lacions, servidors, sistemes i personal implicat.

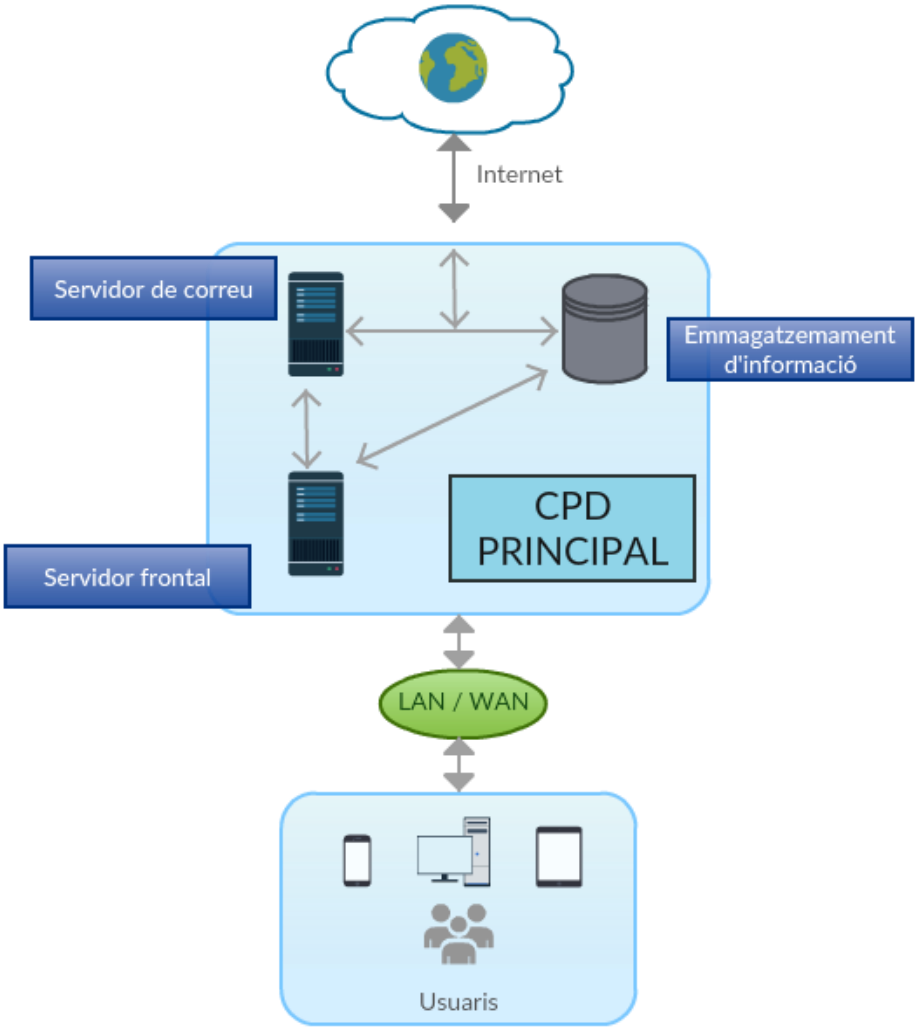

Figura 10. Arquitectura original del correu corporatiu de la organització (Elaboració pròpia)

9.4 Anàlisi de riscos

Per realitzar l'anàlisi de riscos de l'escenari plantejat s'utilitzarà una metodologia que combina l'anàlisi qualitatiu i quantitatiu i que es troba explicada amb més detall al treball de la Laura Abellanet. Aquesta metodologia segueix 7 fases principals per tal d'obtenir el nivell de risc:

- **Fase 1:** Identificació d'actius
- **Fase 2:** Resultats de l'anàlisi d'impacte de la solució
- **Fase 3:** Amenaces i avaluació de la probabilitat
- **Fase 4:** Anàlisi del risc inherent
- **Fase 5:** Identificació del marc de controls a implementar
- **Fase 6:** Càlcul del nivell de cobertura
- **Fase 7:** Càlcul del risc residual

Un cop obtingut aquest nivell de risc, es comentaran els resultats i es detallaran els riscos obtinguts.

9.4.1 Fase 1: Identificació d'actius a protegir

L'anàlisi, com s'ha comentat a la definició de l'entorn, cobrirà el servei de correu on-premise d'una organització i el seu propi sistema d'emmagatzemament de dades. Cal destacar que aquests dos actius coincideixen amb la seva versió cloud, l'Exchange d'Office365 i el One Drive, que són els que ha analitzat la Laura Abellanet al seu treball.

9.4.2 Fase 2: Anàlisi d'impacte de la solució

Un cop identificats els actius, es realitzarà un anàlisi d'impacte que, al no considerar de moment cap tipus de control, serà comú tant per la opció on-premise com per la opció cloud.

L'objectiu d'aquesta part serà valorar quin impacte tindria sobre l'organització el compromís en la seguretat dels actius a analitzar. Aquest compromís s'analitzarà des del punt de vista de la confidencialitat, la integritat i la disponibilitat dels actius i considerarà els següents tipus d'impacte:

- **Econòmic:** Indicarà el cost i les pèrdues que l'incident suposarà a l'organització.
- **Operacional:** Indicarà el grau d'afectació sobre els processos i sistemes de l'empresa.
- **Legal:** Determinarà la magnitud de les conseqüències que tindrà l'incident a nivell legal i regulatori.
- **Reputacional:** Indicarà els danys que suposaria un incident de cara a la confiança i la opinió de la societat cap a l'empresa.

És cert que tots aquests impactes són considerables però no tots ells tenen el mateix pes o les mateixes conseqüències per les organitzacions, ja que els impactes econòmic i legal suposen unes pèrdues bastant més elevades que la resta. És per això que s'han assignat els següents pesos a cadascun d'ells:

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

Finalment, es definirà l'escala utilitzada per realitzar el càlcul d'impacte, per la que s'han considerat els següents nivells:

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

Un cop amb els valors, s'han analitzat els límits per canviar de nivell a cadascun dels tipus d'impacte. En aquest sentit destaquem,

- A nivell econòmic, 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 agafat com a límit les dues hores per considerar que l'impacte operacional és baix. 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 utilitzada:

Valor	Impacte	Reputacional	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 des habilitat / Interrupció total de les operacions / Temps de recuperació de més d'1 dia

Taula 3. Escala d'impactes

Un cop definits els diferents nivells per cada impacte, s'analitzarà cadascuna de les àrees de seguretat:

Confidencialitat

Impacte Confidencialitat (IC)	Impacte econòmic (IE)	Impacte de Reputació (IR)	Impacte Legal (IL)	Impacte operacional (IO)	Racional
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.

Taula 4. Càlcul de l'impacte en la confidencialitat

Integritat

Impacte Integritat (II)	Impacte econòmic (IE)	Impacte de Reputació (IR)	Impacte Legal (IL)	Impacte operacional (IO)	Racional
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.

Taula 5. Càlcul de l'impacte en la integritat

Disponibilitat

Impacte Disponibilitat (ID)	Impacte econòmic (IE)	Impacte de Reputació (IR)	Impacte Legal (IL)	Impacte operacional (IO)	Racional
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.

Taula 6. Càlcul de l'impacte en la disponibilitat

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

CONFIDENCIALITAT						
Actius	**Impacte Confidencialitat (IC)**	**Impacte econòmic (IE)**	**Impacte de Reputació (IR)**	**Impacte Legal (IL)**	**Impacte operacional (IO)**	**Racional**
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 l'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, la exposició d'alguna informació del correu electrònic podria suposar impacte legal i de reputació.
Storage	**3,8**	4	4	5	3	Al comprometre la confidencialitat es podrien donar accessos a informació sensible de l'organització per part d'usuaris no autoritzats o d'atacants externs.

Taula 7. Impacte sobre la confidencialitat aplicat al servei de correu

INTEGRITAT						
Actius	**Impacte Integritat (II)**	**Impacte econòmic (IE)**	**Impacte de Reputació (IR)**	**Impacte Legal (IL)**	**Impacte operacional (IO)**	**Racional**
Exchange	**3,0**	3	3	3	3	Davant la pèrdua o la modificació no autoritzada de les dades, la operativa de l'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.
Storage	**3,0**	3	3	3	3	Davant la pèrdua o la modificació no autoritzada de les dades, la operativa de l'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 8. Impacte sobre la integritat aplicat al servei de correu

DISPONIBILITAT						
Actius	**Impacte Disponibilitat (ID)**	**Impacte econòmic (IE)**	**Impacte de Reputació (IR)**	**Impacte Legal (IL)**	**Impacte operacional (IO)**	**Racional**
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.
Storage	**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.

Taula 9. Impacte sobre la disponibilitat aplicat al servei de correu

Finalment 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:

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

Taula 10. Taula resum d'impactes sobre el correu corporatiu

9.4.3 Fase 3: Amenaces i avaluació de la probabilitat

Un cop coneixem l'impacte que tindria un incident de seguretat sobre els actius a estudiar, es buscaran les amenaces que apliquen a l'organització i al servei de correu en concret i s'avaluarà la seva probabilitat d'ocurrència.

Per categoritzar les probabilitats s'utilitzarà la següent escala:

Probabilitat	Definició
Molt baixa (1)	Pràcticament impossible que es materialitzi
Baixa (2)	Es pot materialitzar en els propers 10 anys
Mitja (3)	Es pot materialitzar en els propers 2-3 anys
Alta (4)	Es pot materialitzar abans d'un any
Molt Alta (5)	Es pot materialitzar en els propers mesos

Taula 11. Escala de probabilitats

A continuació es mostren les principals amenaces de seguretat a les que s'exposen les organitzacions, extretes de l'informe anual d'EINSA de 2017 i del llistat d'amenaces d'ISACA. Entendrem que, al tractar-se de les amenaces més comuns, totes elles tindran una probabilitat molt alta d'ocurrència:

Amenaces	Descripció	Probabilitat
Fuga d'informació	La fuga d'informació és una de les principals preocupacions de les organitzacions, que veuen que cada any augmenten els incidents d'aquest tipus. Són moltes les tipologies d'informació utilitzades (dades personals, dades de targetes, propietat intel·lectual, estats financers...) i els canals pels que aquesta informació es pot filtrar, ja sigui de forma intencionada o involuntària.	**Molt alta**
Pobre gestió d'identitats, credencials i accessos	Actualment els usuaris tenen accessos a multitud d'aplicacions, comptes, carpetes i recursos. En organitzacions amb un gran nombre d'usuaris, és complexe controlar qui accedeix a quins recursos, com hi accedeix i durant quant temps.	**Molt alta**

Vulnerabilitats de sistema i aplicació	Tots els sistemes tenen vulnerabilitats, que en menor o major mida, poden posar en risc les dades i el servei que ofereixen. Si no s'apliquen mesures i actualitzacions freqüents, les vulnerabilitats suposen una gran amenaça	**Molt alta**
Atacants maliciosos	És molt probable que una organització tingui gent o grups que, seguint diverses motivacions, vulguin perjudicar-la o danyar-la. El nombre d'atacants no ha parat de creixes durant els últims anys i els atacs són cada cop més sofisticats i difícils d'identificar.	**Molt alta**
Pèrdua d'informació i de servei	Una organització ha de vetllar per prestar el seu servei amb les mínimes aturades possibles, però no es pot permetre perdre dades. Hi ha molts factors que podrien provocar aquesta pèrdua com poden ser catàstrofes naturals i desastres, errors en els sistemes, atacs deliberats o destrucció de dades de forma no intencionada.	**Molt alta**
Mala gestió de les dades per part dels proveïdors	Les organitzacions grans acostumen a delegar la gestió de molts dels seus serveis a proveïdors externs. També comparteixen les seves dades, cosa que requereix que els proveïdors compleixin uns certs requeriments a per garantir que aquestes s'utilitzen i s'emmagatzemen de forma segura.	**N/A**
Errors humans i configuracions incorrectes	Els treballadors d'una organització i els administradors de seguretat són humans i els humans no som perfectes. És per això que els errors i les configuracions incorrectes de sistemes, capacitats de seguretat, dispositius i d'altres recursos són molt probables en entorns tant complexes i gestionats per tantes persones	**Molt alta**
Infecció de programari maliciós	De programari maliciós n'hi ha de tota mena; virus, malware, cucs, troians, bombes lògiques i d'altres formes de codi maliciós. Tota prevenció és poca per part de les organitzacions de cara a assegurar-se de que no són infectades per aquest programari.	**Molt alta**

Manca de traçabilitat d'accions sobre els sistemes	Els entorns empresarials són complexes, estan formats per multitud de xarxes i sistemes i per molts dispositius que interactuen entre ells. Si l'organització no és capaç d'identificar incidents, monitoritzar la xarxa i portar una traçabilitat de la informació generada pels seus sistemes, no podrà actuar contra cap tipus d'esdeveniment.	**Molt alta**

Taula 12. Principals amenaces de seguretat actuals

Cal destacar que de les principals amenaces de seguretat, no aplica la mala gestió de les dades per part dels proveïdors perquè en el cas que estem tractant no hi ha cap proveïdor que gestioni el servei, ja que tot es porta de manera interna.

9.4.4 Fase 4: Anàlisi del risc inherent

Com s'ha explicat a la part teòrica del treball, el risc es calcula multiplicant l'impacte d'una amenaça per la probabilitat de que es materialitzi. Per tant, tenint ja els impactes i probabilitats, podem calcular el risc inherent. Cal recordar que aquest risc és el que hi hauria en cas de no considerar cap control de seguretat, per tant serà previsiblement bastant alt. Un cop tinguem aquest risc inherent, l'objectiu serà implementar controls de seguretat per reduir-lo.

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

Seguint aquesta relació, podem veure els diferents nivells de risc a les següents taules:

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**

Taula 13. Càlcul del risc inherent en funció de l'impacte i la probabilitat

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

Taula 14. Escala de valors pel risc inherent

Seguint aquesta escala, a continuació es mostren els resultats obtinguts al analitzar els impactes que suposaria cadascuna de les amenaces identificades:

		Confidencialitat			Integritat			Disponibilitat		
Amenaça	**Probabilitat**	**Impacte Conf.**	**Risc Conf.**	**Risc inherent**	**Impacte Int.**	**Risc Int.**	**Risc inherent**	**Impacte Disp.**	**Risc Disp.**	**Risc inherent**
Fuga d'informació	5	3,8	19,2	Alt	N/A	N/A	N/A	N/A	N/A	N/A
Pobre gestió d'identitats, credencials i accessos	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
Vulnerabilitats de sistema i aplicació	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
Atacants maliciosos	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
Pèrdua d'informació i de servei	5	N/A	N/A	N/A	3,0	15,0	Alt	4,3	21,7	Molt Alt
Errors humans i configuracions incorrectes	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
Infecció de programari maliciós	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt
Manca de traçabilitat d'accions sobre els sistemes	5	3,8	19,2	Alt	3,0	15,0	Alt	4,3	21,7	Molt Alt

Taula 15. Risc inherent derivat de les principals amenaces de seguretat

Com a comentari de l'anàlisi, no s'ha considerat impacte en la integritat i la disponibilitat en cas de que es produeixi una fuga d'informació, ja que aquesta amenaça aplica únicament a la confidencialitat. De la mateixa manera l'impacte en la confidencialitat no aplica a la amenaça de pèrdua d'informació i servei.

Podem veure, com s'ha comentat, que els nivells de risc són comprensiblement alts o molt alts ja que el risc inherent no considera cap control de seguretat implementat.

9.4.5 Fase 5: Identificació del marc de controls a implementar

Un cop obtingut el nivell de risc inherent, l'objectiu serà definir una sèrie de controls o salvaguardes de seguretat per tal de reduir-lo i obtenir finalment un risc residual com més baix millor. Existeixen molts marcs de controls de seguretat definits per aplicar a les organitzacions, en aquest cas s'han agafat com a base els controls publicats pel NIST (versió 1.1, Abril de 2018). Aquest marc de controls està orientat principalment a grans organitzacions de banca, energia, comunicacions i fins i tot organismes governamentals i defensa.

Figura 10. Àmbits d'aplicació del marc de controls NIST (NIST, 2018)

Aquest marc divideix els seus controls en cinc grans grups, corresponents a cinc accions considerades principals per garantir la seguretat: Identificar, Protegir, Detectar, Respondre i Recuperar. Dins de cadascuna d'aquestes accions hi ubica els controls de seguretat segons la seva funció.

Cal no oblidar, però, que l'aplicació directa d'un marc de controls predeterminat, per molt complert que aquest sigui, pot obviar requeriments fonamentals de l'organització en funció de la seva naturalesa, mida, activitat de negoci o d'altres aspectes que requereixin controls específics no contemplats en el marc de control. També es molt possible que no tots els controls definits al marc siguin aplicables o necessaris per les raons prèviament comentades. La utilització del marc de controls del NIST ve també donada per la seva flexibilitat i la facilitat que té d'adaptar-se a entorns a més petita escala o a simplement serveis concrets dins d'una gran organització com és el cas d'aquest anàlisi. És per això que no tots aquests controls s'han inclòs a l'anàlisi i alguns d'ells s'han adaptat a l'entorn i al servei sota estudi. Els controls també s'han dividit en àmbits més concrets de la seguretat per simplificar la seva relació amb les amenaces aplicables.

Àmbit d'aplicació
Gestió de les dades i la informació
Gestió d'identitats
Gestió de la infraestructura
Disponibilitat dels sistemes y pèrdua d'informació
Procediments de seguretat
Monitorització i traçabilitat
Seguretat de xarxa i comunicacions

Taula 16. Àmbits d'aplicació del marc de controls

Els controls obtinguts s'han dividit en vuit grans grups, en funció del seu àmbit i la seva tipologia. El proper pas serà identificar quines amenaces mitiguen cadascun dels controls proposats, creuant-los amb el llistat d'amenaces prèviament definit. Cal remarcar que alguns controls són aplicables a més d'una amenaça.

A continuació es mostra el conjunt de controls proposats relacionats amb les amenaces que mitiguen.

		Fuga d'informació	Pobre gestió d'identitats, credencials i accessos	Vulnerabilitats de sistema i aplicació	Atacants maliciosos	Pèrdua de dades i de servei	Errors humans i configuracions incorrectes	Infecció de programari maliciós	Manca de traçabilitat d'accions sobre els sistemes
Àmbit d'aplicació	**Control**								
Gestió de les dades i la informació	S'implementen mecanismes de protecció de dades en repòs	x			x	x			
	S'implementen mecanismes de protecció de dades en trànsit	x			x	x			
	S'han implementat mecanismes de protecció contra la fuga d'informació	x							
	Tots els fitxers adjuntats per l'usuari són escanejats pel sistema antivirus			x	x			x	
	Els entorns de desenvolupament i proves estàn segregats de l'entorn de producció	x						x	
	Es segueix un procediment d'eliminació de dades d'acord amb la regulació	x					x		
Gestió d'identitats	Es gestionen i verifiquen les identitats i les credencials per a dispositius, usuaris i processos		x						
	Tota identitat del sistema està vinculada a unes úniques credencials corresponents a un únic usuari		x						x
	S'utilitzen eines específiques de gestió d'usuaris administradors		x		x				x
Gestió de la infraestructura	S'han implementat mecanismes de seguretat física per accedir als sistemes				x				
	L'accés d'administració dels sistemes està restringit a unes determinades IPs				x				
Disponibilitat dels sistemes y pèrdua d'informació	S'executen còpies de seguretat periòdiques dels sistemes					x			
	S'han definit plans de resposta a incidents, de continuitat de negoci i de DR					x			
	Els sistemes estàn redundats per oferir disponibilitat en cas d'incident					x			
	Els sistemes s'han dissenyat per tal de poder suportar la càrrega de dades del servei					x			
	S'utilitzen eines de protecció davant d'atacs de denegació de servei (DoS)					x			

Taula 17. Marc de controls aplicable a les principals amenaces de seguretat

		Fuga d'informació	Pobre gestió d'identitats, credencials i accessos	Vulnerabilitats de sistema i aplicació	Atacants maliciosos	Pèrdua de dades i de servei	Errors humans i configuracions incorrectes	Infecció de programari maliciós	Manca de traçabilitat d'accions sobre els sistemes
Àmbit d'aplicació	**Control**								
Procediments de seguretat	Tots els dispositius, sistemes, aplicacions i plataformes que composen el sistema han de ser inventariats								x
	Es segueix un programa de formació i conscienciació en matèria de seguretat						x		
	Es segueixen guíes de bastionat per realitzar les configuracions dels sistemes						x		
	S'ha definit un procés de gestió de canvis i configuracions						x		
	S'ha desenvolupat i implementat un pla de gestió de vulnerabilitats			x					
	S'executen escanejos de vulnerabilitats periòdics sobre els sistemes			x					
	S'executen pentests periódics sobre els sistemes			x					
	S'han identificat i documentat les vulnerabilitats dels sistemes			x					
Monitorització i traçabilitat	Els logs generats pels diferents sistemes i sensors s'emmagatzemaràn dins d'una única solució de monitorització								x
	Es generaràn alertes per tal d'identificar accions malicioses als sistemes								x
	La xarxa es monitoritza per detectar potencials esdeveniments de ciberseguretat								x
	L'entorn físic es monitoritza per detectar potencials esdeveniments de ciberseguretat								x
	L'activitat del personal es monitoritza per detectar potencials events de ciberseguretat								x
	Es monitoritza l'accés de personal, les connexions i els dispositius utilitzats								x
Seguretat de xarxa i comunicacions	Les xarxes estàn segregades per tal de protegir la seva integritat	x							
	Es restringeix l'ús de dispositius d'emmagatzemament extraible	x			x			x	
	S'utilitzen eines de detecció de codi maliciòs				x			x	
	Les comunicacions amb tercers estàn xifrades	x			x				

Taula 18. Marc de controls aplicable a les principals amenaces de seguretat (continuació)

9.4.6 Fase 6: Càlcul del nivell de cobertura

El grau de cobertura que proporciona cada control vindrà donat per la seva efectivitat de cara a mitigar el risc que suposen les amenaces a les que apliqui. Òbviament, no proporcionarà la mateixa cobertura realitzar cursos de conscienciació sobre seguretat als treballadors de l'organització que implementar un pla de gestió de vulnerabilitats i realitzar escaneigs periòdics. Per classificar els graus de cobertura s'utilitzarà la següent escala:

Cobertura
Molt Alta
Alta
Mitjana
Baixa

Taula 19. Escala de nivells de cobertura

Un cop conegut el grau de cobertura de cada control, s'avaluarà la cobertura total per a cadascuna de les amenaces identificades, tenint en compte que hi ha controls que apliquen a més d'una amenaça. Com més controls apliquin a una amenaça i com més forts siguin aquests, major serà el grau de cobertura.

9.4.7 Fase 7: Càlcul del risc residual

Com s'ha comentat al marc teòric, siguin quines siguin les solucions de seguretat, sempre quedarà un cert nivell de risc, anomenat risc residual. L'últim pas de l'anàlisi consistirà en calcular aquest risc, que es defineix com el nivell de risc que no ha sigut mitigat per cap control i que no ha aconseguit ser reduït per cap salvaguarda.

El risc residual es defineix com:

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

Veiem doncs que, amb el risc inherent calculat a la Fase 4 i el nivell de cobertura obtingut a la fase 6, ja disposem de tots els factors per calcular-lo. Per fer-ho s'ha utilitzat la següent escala, que considera 5 nivells de risc:

Risc Residual
Molt baix
Baix
Mitjà
Alt
Molt Alt

Taula 20. Escala de valors pel risc residual

A la següent taula es pot veure aquest nivell de risc residual en funció del nivell de risc inherent i cobertura:

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**

Taula 21. Càlcul del risc residual en funció del risc inherent i la cobertura

Un cop definida l'escala, es disposa de tots els factors per calcular el risc residual. A la següent taula es poden veure tots els controls proposats, la cobertura que suposen de cara a mitigar l'amenaça a la que apliquen i el risc residual obtingut per a cadascun dels tres dominis de la seguretat (confidencialitat, integritat i disponibilitat):

						Confidencialitat		Integritat		Disponibilitat	
ID Amenaça	**Amenaça**	**ID Control**	**Control**	**Cobertura Controls**	**Cobertura Total**	**Risc Inherent**	**Risc Residual**	**Risc Inherent**	**Risc Residual**	**Risc Inherent**	**Risc Residual**
A1	**Fuga d'informació**	C.1	S'implementen mecanismes de protecció de dades en repòs	Mitjana	**Mitjana**	**Alt**	**Mitjà**	**N/A**	**N/A**	**N/A**	**N/A**
		C.2	S'implementen mecanismes de protecció de dades en trànsit	Mitjana							
		C.3	S'han implementat mecanismes de protecció contra la fuga d'informació	Alta							
		C.5	Els entorns de desenvolupament i proves estàn segregats de l'entorn de producció	Mitjana							
		C.6	Es segueix un procediment d'eliminació de dades d'acord amb la regulació	Mitjana							
		C.31	Les xarxes estàn segregades per tal de protegir la seva integritat	Alta							
		C.32	Es restringeix l'ús de dispositius d'emmagatzemament extraible	Mitjana							
		C.34	Les comunicacions amb tercers estàn xifrades	Alta							
A2	**Pobre gestió d'identitats, credencials i accessos**	C.7	Es gestionen i verifiquen les identitats i les credencials per a dispositius, usuaris i processos	Molt Alta	**Molt Alta**	**Alt**	**Molt baix**	**Alt**	**Molt baix**	**Molt alt**	**Baix**
		C.8	Tota identitat del sistema està vinculada a unes úniques credencials corresponents a un únic usuari	Alta							
		C.9	S'utilitzen eines específiques de gestió d'usuaris administradors	Molt alta							
A3	**Vulnerabilitats de sistema i aplicació**	C.4	Tots els fitxers adjuntats per l'usuari són escanejats pel sistema antivirus	Alta	**Molt Alta**	**Alt**	**Molt baix**	**Alt**	**Molt baix**	**Molt alt**	**Baix**
		C.21	S'ha desenvolupat i implementat un pla de gestió de vulnerabilitats	Molt Alta							
		C.22	S'executen escanejos de vulnerabilitats periòdics sobre els sistemes	Molt Alta							
		C.23	S'executen pentests periódics sobre els sistemes	Molt Alta							
		C.24	S'han identificat i documentat les vulnerabilitats dels sistemes	Alta							
A4	**Atacants maliciosos**	C.1	S'implementen mecanismes de protecció de dades en repòs	Alta	**Alta**	**Alt**	**Baix**	**Alt**	**Baix**	**Molt alt**	**Mitjà**
		C.2	S'implementen mecanismes de protecció de dades en trànsit	Alta							
		C.4	Tots els fitxers adjuntats per l'usuari són escanejats pel sistema antivirus	Alta							
		C.9	S'utilitzen eines específiques de gestió d'usuaris administradors	Alta							
		C.10	S'han implementat mecanismes de seguretat física per accedir als sistemes	Alta							
		C.11	L'accés d'administració dels sistemes està restringit a unes determinades IPs	Mitjana							
		C.32	Es restringeix l'ús de dispositius d'emmagatzemament extraible	Alta							
		C.33	S'utilitzen eines de detecció de codi maliciòs	Alta							
		C.34	Les comunicacions amb tercers estàn xifrades	Molt Alta							

Taula 22. Anàlisi de riscos

						Confidencialitat		Integritat		Disponibilitat	
ID Amenaça	**Amenaça**	**ID Control**	**Control**	**Cobertura Controls**	**Cobertura Total**	**Risc Inherent**	**Risc Residual**	**Risc Inherent**	**Risc Residual**	**Risc Inherent**	**Risc Residual**
A5	**Pèrdua de dades i de servei**	C.1	S'implementen mecanismes de protecció de dades en repòs	Alta	**Alta**	**N/A**	**N/A**	**Alt**	**Baix**	**Molt alt**	**Mitjà**
		C.2	S'implementen mecanismes de protecció de dades en trànsit	Alta							
		C.12	S'executen còpies de seguretat periòdiques dels sistemes	Alta							
		C.13	S'han definit plans de resposta a incidents, de continuitat de negoci i de DR	Alta							
		C.14	Els sistemes estàn redundats per oferir disponibilitat en cas d'incident	Alta							
		C.15	Els sistemes s'han dissenyat per tal de poder suportar la càrrega de dades del servei	Alta							
		C.16	S'utilitzen eines de protecció davant d'atacs de denegació de servei (DoS)	Mitjana							
A6	**Errors humans i configuracions incorrectes**	C.6	Es segueix un procediment d'eliminació de dades d'acord amb la regulació	Alta	**Alta**	**Alt**	**Baix**	**Alt**	**Baix**	**Molt alt**	**Mitjà**
		C.18	Es segueix un programa de formació i conscienciació en matèria de seguretat	Mitjana							
		C.19	Es segueixen guíes de bastionat per realitzar les configuracions dels sistemes	Alta							
		C.20	S'ha definit un procés de gestió de canvis i configuracions	Alta							
A7	**Infecció de programari maliciós**	C.4	Tots els fitxers adjuntats per l'usuari són escanejats pel sistema antivirus	Alta	**Alta**	**Alt**	**Baix**	**Alt**	**Baix**	**Molt alt**	**Mitjà**
		C.5	Els entorns de desenvolupament i proves estàn segregats de l'entorn de producció	Mitjana							
		C.32	Es restringeix l'ús de dispositius d'emmagatzemament extraible	Alta							
		C.33	S'utilitzen eines de detecció de codi maliciòs	Alta							
A8	**Manca de traçabilitat d'accions sobre els sistemes**	C.8	Tota identitat del sistema està vinculada a unes úniques credencials corresponents a un únic usuari	Alta	**Molt Alta**	**Alt**	**Molt baix**	**Alt**	**Molt baix**	**Molt alt**	**Baix**
		C.9	S'utilitzen eines específiques de gestió d'usuaris administradors	Alta							
		C.17	Tots els dispositius, sistemes, aplicacions i plataformes que composen el sistema han de ser inventariats	Alta							
		C.25	Els logs generats pels diferents sistemes i sensors s'emmagatzemaràn dins d'una única solució de monitorització	Molt Alta							
		C.26	Es generaràn alertes per tal d'identificar accions malicioses als sistemes	Molt Alta							
		C.27	La xarxa es monitoritza per detectar potencials esdeveniments de ciberseguretat	Molt Alta							
		C.28	L'entorn físic es monitoritza per detectar potencials esdeveniments de ciberseguretat	Molt Alta							
		C.29	L'activitat del personal es monitoritza per detectar potencials events de ciberseguretat	Molt Alta							
		C.30	Es monitoritza l'accés de personal, les connexions i els dispositius utilitzats	Molt Alta							

Taula 23. Anàlisi de riscos (continuació)

A continuació es mostra la taula resum amb el risc residual resultant per a cada amenaça i domini:

	Confidencialitat	Integritat	Disponibilitat
Amenaça	**Risc Residual**	**Risc Residual**	**Risc Residual**
Fuga d'informació	**Mitjà**	**N/A**	**N/A**
Pobre gestió d'identitats, credencials i accessos	**Molt baix**	**Molt baix**	**Baix**
Vulnerabilitats de sistema i aplicació	**Molt baix**	**Molt baix**	**Baix**
Atacants maliciosos	**Baix**	**Baix**	**Mitjà**
Pèrdua de dades i de servei	**N/A**	**Baix**	**Mitjà**
Errors humans i configuracions incorrectes	**Baix**	**Baix**	**Mitjà**
Infecció de programari maliciós	**Baix**	**Baix**	**Mitjà**
Manca de traçabilitat d'accions sobre els sistemes	**Molt baix**	**Molt baix**	**Baix**

Taula 24. Resultats de l'anàlisi de riscos

Els resultats permeten veure que s'ha pogut reduir el risc residual en gran mesura, tenint principalment valors baixos de risc. Era previsible que els resultats siguin satisfactoris en aquest sentit ja que el marc de controls proposat s'ha adaptat al servei a analitzar i també a que s'ha considerat que tots els controls proposats són aplicables. En un entorn real això no serà sempre possible ja que sovint hi ha controls que presenten grans dificultats en la seva implementació, ja sigui pel seu cost, la seva complexitat o d'altres factors.

Un cop implementats els controls identificats, l'entorn a securitzar presentat a l'inici de l'anàlisi presenta bastants canvis, detallats a continuació:

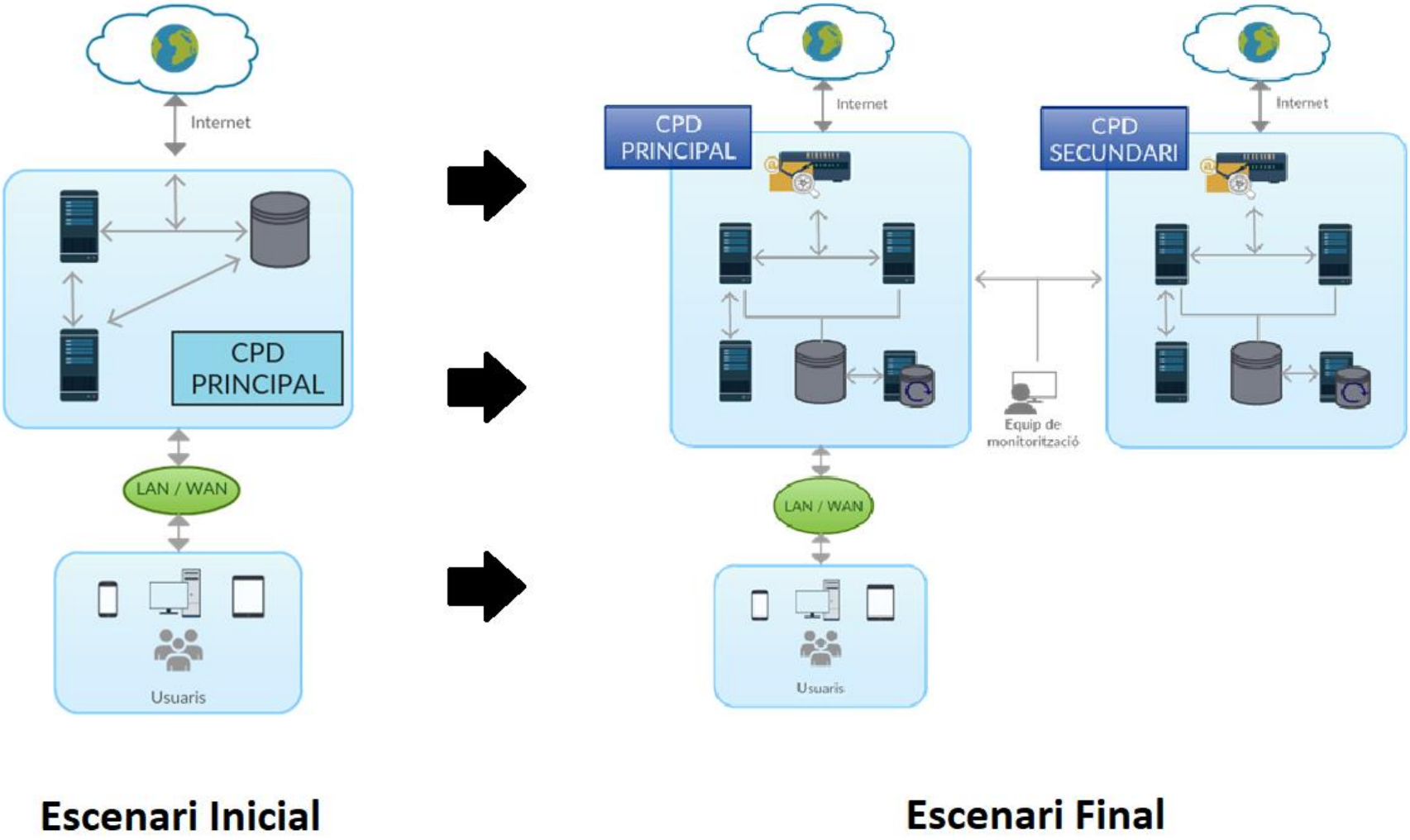

Figura 11. Arquitectura final del correu corporatiu de la organització (Elaboració pròpia)

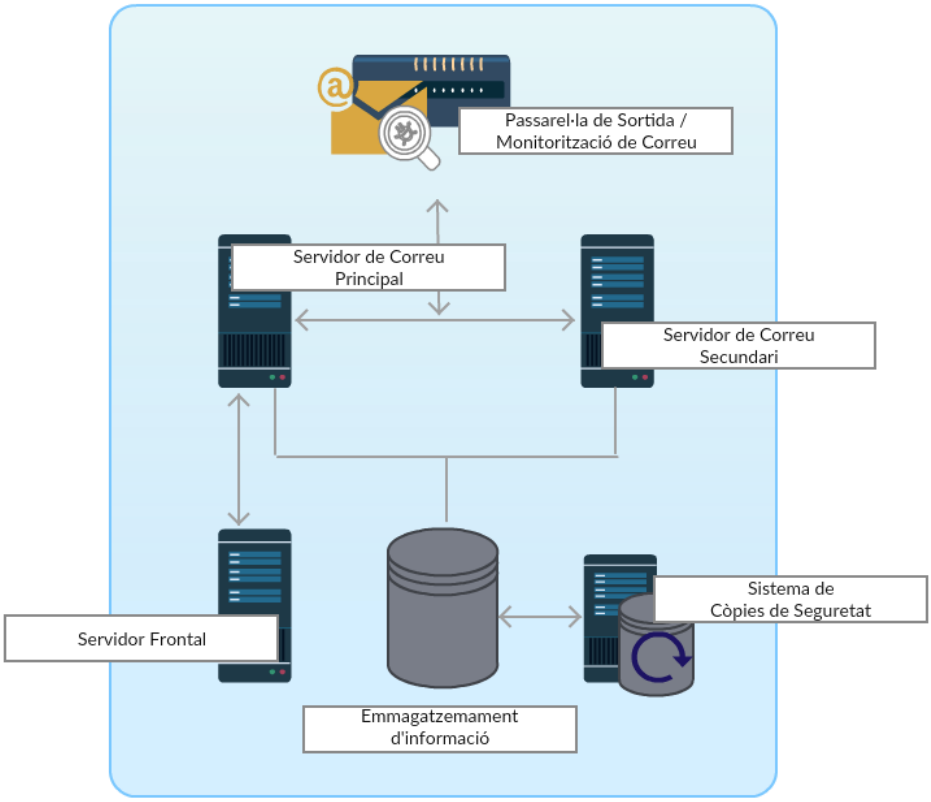

Figura 12. Arquitectura del CPD (Elaboració pròpia)

- S'ha replicat tota la infraestructura dins d'un Centre de Processament de Dades secundari que actua com a contingència del centre principal. En cas d'un incident al CPD principal, tot el servei es podria seguir oferint des del secundari.
- Dins del mateix CPD també s'ha replicat el servidor de correu, per oferir redundància de centre. En cas d'averia o compromís d'un dels servidors, l'altre podria seguir donant servei sense haver de bascular al CPD secundari.
- S'ha incorporat una passarel·la que inclou totes les capacitats de seguretat per tal de monitoritzar el correu entrant i sortint.
- S'ha incorporat una solució de monitorització en temps real que permet que l'equip de seguretat de la entitat analitzi el funcionament del servei en tot moment.
- La solució d'emmagatzemament compta ara amb un sistema de back-ups que realitza còpies de seguretat periòdiques.

Tenim d'aquesta manera un entorn molt més robust davant possibles caigudes i incidents, amb un alt nivell de monitorització i capacitats de seguretat. Juntament amb l'aplicació de la resta de controls proposats, podem parlar d'una millora considerable a nivell de seguretat i una gran disminució del risc.

Tot i els resultats satisfactoris, tenim un nivell de risc residual que es manté i s'han d'analitzar les seves causes. Per realitzar aquest estudi analitzarem la situació de cadascuna de les amenaces un cop implementats els controls:

Amenaça	Risc Residual	Descripció
Fuga d'informació	**Mitjà**	**Tot i les mesures implementades per evitar la fuga de dades, la naturalesa del servei de correu corporatiu fa molt difícil evitar-la per complert. Els usuaris podrien enviar correus amb text o amb documents adjunts que evitin el DLP i es filtrin dades sensibles a l'exterior.**
Pobre gestió d'identitats, credencials i accessos	Molt baix	Els usuaris han d'autenticar-se amb un usuari personal únic i amb una contrasenya robusta per tal d'accedir al sistema. En cas de que un usuari maliciós aconseguís accés a un usuari que no sigui el seu, les seves accions estarien molt limitades pels permisos assignats i la naturalesa del servei de correu electrònic. L'accés malintencionat a un usuari administrador si que podria suposar greus conseqüències però és molt remota al disposar la entitat d'un sistema de gestió d'usuaris administradors (PAM).
Vulnerabilitats de sistema i aplicació	Molt baix	L'organització ha definit un sistema de gestió de vulnerabilitats i executa escaneigs periòdics per detectar-les. També es disposa de l'avantatge de controlar tot l'entorn i conèixer perfectament quines màquines, servidors i dispositius constitueixen el sistemes. Tot i que, com ja s'ha comentat, la existència de vulnerabilitats als sistemes és inevitable, la execució d'aquests escaneigs i la resolució pautada i programada fan que el risc de que s'explotin sigui baix.
Atacants maliciosos	**Baix**	**Els controls per neutralitzar atacs informàtics són diversos i molts d'ells molt efectius. Tot i això, les empreses d'avui en dia s'enfronten a veritables organitzacions criminals que executen sovint atacs molt complexes i planificats (com per exemple els APT) i fan que no es pugui descartar el risc de ser objectius d'un atac d'aquestes característiques per moltes mesures que s'apliquin.**

Pèrdua d'informació i de servei	**Baix**	**La redundància de centre (dins d'un CPD) i entre dos CPD ofereix una alta garantia de disponibilitat del servei. Tot i això, no es pot descartar el risc de que una catàstrofe natural, un atac a gran escala o un altre conjunt de factors inhabilitin els sistemes i es produeixi una caiguda o una possible pèrdua de dades.**
Errors humans i configuracions incorrectes	**Baix**	**Els treballadors i el personal de seguretat d'una empresa són humans i els humans cometem errors. Per tal de reduir possibles configuracions incorrectes de dispositius, s'han definit guies de bastionat de sistemes i s'han programat esdeveniments de formació en seguretat pel personal de l'empresa. Tot i això, l'ésser humà és el punt més dèbil al parlar de seguretat i cal tenir en compte aquest risc.**
Infecció de programari maliciós	**Baix**	**Tot i les capacitats de seguretat implementades, ni tant sols els dispositius antivirus i antimalware més potents són capaços de detectar alguns tipus de programari maliciós. És per això que existeix un cert risc de ser infectats i no es pot descartar aquesta amenaça.**
Manca de traçabilitat d'accions sobre els sistemes	Molt baix	S'han implementat diverses mesures per monitoritzar els sistemes, es recullen es logs generats en una única solució de monitorització i es defineixen alertes per detectar comportaments sospitosos. Aquest alt nivell de monitorització i el fet de que l'entorn és reduït fan poc probable que es produeixin incidents o accions no identificades.

Taula 25. Riscos identificats per les principals amenaces de seguretat

Finalment, traurem d'aquest anàlisi la foto de riscos per l'escenari plantejat:

Risc	Descripció del risc
Fuga d'informació	Fuga de dades sensibles i informació confidencial a través del correu electrònic
Atacs maliciosos	Possibilitat de rebre un atac avançat sobre els sistemes d'informació.
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
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 malicios

Taula 26. Principals riscos identificats

Veiem que el resultat final són cinc riscos, un de classificació mitjana i quatre de nivell baix. Amb aquesta informació es conclou l'anàlisi de riscos i el següent pas seria presentar-lo a l'alta direcció de l'organització.

Un cop vistos els resultats, aquesta capa de direcció serà l'encarregada de decidir què fer amb els riscos, poden sol·licitar mitigar-los o transferir-los, per tant s'haurien de dedicar recursos addicionals per reduir encara més el nivell de risc o poden acceptar-los i entendre que l'organització realitzarà la seva operativa sota l'amenaça d'aquests riscos.

9.5 Comparativa amb la solució Cloud

Un cop realitzat l'anàlisi de riscos per les solucions on-premise i cloud, es compararan els resultats per veure quins són els riscos comuns per les dues solucions, quins riscos específics presenten els dos paradigmes i els aspectes de millora per a cadascun d'ells. La comparativa realitzada dins d'aquest apartat utilitza els resultats presentats per la Laura Abellanet al seu treball *"Anàlisi de la ciberseguretat en la migració cap a entorns cloud",* en el que s'han obtingut els següents riscos per la solució de correu corporatiu al 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)	

Taula 27. Riscos identificats per la solució cloud

Pel que fa als riscos en comú per les dues solucions, trobem que el principal risc és la fuga d'informació. En general les solucions DLP són més robustes als sistemes on-premise, principalment perquè al tenir un control total sobre la xarxa interna, poden ser fàcilment adaptades a les necessitats de l'organització a protegir, controlant tot el tràfic d'informació dins i cap a fora de la xarxa. Tot i això, la naturalesa del servei de correu corporatiu fa molt difícil evitar la fuga d'informació per complert. Els usuaris podrien enviar correus amb text o amb documents adjunts que evitin el DLP i es filtrin dades sensibles a l'exterior.

A la solució cloud, aquest risc és encara més elevat quan s'accedeix de manera directa a l'Office 365 sense passar per la xarxa corporativa, donant la possibilitat a un empleat d'emmagatzemar informació confidencial dins dels seus propis dispositius. Aquest risc es mitiga en certa mesura quan la connexió es produeix a través de la xarxa corporativa, podent aplicar controls solucions de prevenció contra la fuga d'informació dins del CPD.

La flexibilitat que ofereixen les solucions cloud, i que les han fet tant populars, també comporten els principals riscos de seguretat en comparació amb els sistemes on-premise. La possibilitat d'accedir a Office 365 des de qualsevol xarxa i qualsevol dispositiu fa que existeixi la possibilitat de que s'interceptin les dades en trànsit en cas que les xarxes no siguin segures o de que els dispositius personals presentin vulnerabilitats explotables. Malgrat que l'entorn on-premise està més controlat, aquest també presenta riscos pel que fa a vulnerabilitats als sistemes, necessitant seguir un pla estricte per resoldre-les davant el risc d'atacs maliciosos i infecció de programari.

Pel que fa a la disponibilitat i a la pèrdua d'informació, la solució d'Office 365 presenta la gran avantatge de tenir els seus servidors a CPDs redundats i distribuïts per diferents punts del món. Això permet a Microsoft garantir uns nivells molt alts de disponibilitat que són molt complicats d'igualar per cap altra organització. Per això, en cas de que es produeixi un desastre natural o un atac a gran escala, tot i la redundància plantejada, els sistemes on-premise seran més sensibles i presentaran un risc més elevat de pèrdua de servei i de dades.

A nivell de monitorització, tornem a veure com la solució on-premise presenta més avantatges que el model cloud. Tot i que existeixen eines per monitoritzar i analitzar logs al cloud, hi ha logs que presenten una gran dificultat per ser controlats, com per exemple els generats pels dispositius personals o els generats als sistemes on l'usuari no tingui permisos. 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 generats. D'altra banda, a la solució on-premise, al tenir el control total de tots els sistemes de la organització, és possible analitzar en profunditat tot el que succeeix a l'entorn.

Malgrat les diferències notables a nivell de riscos, la naturalesa dels controls implementats és similar per als dos models. Cal destacar que molts dels controls de la solució on-premise no s'implementen al model cloud ja que venen donats per contracte per part del proveïdor, formant part del servei proporcionat. Així doncs, els controls implementats al cloud estan principalment relacionats amb el control d'accessos, la gestió de vulnerabilitats, els sistemes anti-malware i la traçabilitat, aspectes que també veiem al marc de control on-premise. Veiem així que el que canvia principalment entre els dos models són les eines utilitzades per implementar els controls proposats.

10 Conclusions

10.1 Dificultats durant la realització del treball

Un cop realitzat el marc teòric i el cas pràctic del treball, una de les dificultats principals amb les que ens hem trobat ha sigut intentar abordar un camp tant ampli com la ciberseguretat dins de dos treballs (el de la Laura i el meu). El que anomenem ciberseguretat i seguretat de la informació es composen per moltíssims dominis i explicar cadascun d'ells ja podria perfectament ser el tema d'un únic treball. Per això intentar incloure la informació essencial per donar una visió general del tema ha sigut una de les tasques més complexes.

Pel que fa al cas pràctic, també ha suposat un repte adaptar el marc de controls genèric escollit (el NIST 1.1) a l'entorn sota estudi, ja que tot i que es tracta d'un dels marcs més flexibles que existeixen i és adaptable a tot tipus d'organitzacions i entorns, no ha sigut fàcil reestructurar tots els controls, adaptar-los a l'escenari plantejat i, perquè no dir-ho també, traduir-los de l'anglès al català.

Finalment, una dificultat amb la que no comptàvem al plantejar la idea de definir un marc de controls i fer un anàlisi de riscos és que no disposem d'un entorn real on provar l'aplicabilitat d'aquests controls i per tant els resultats obtinguts dins de l'anàlisi pràctic són essencialment teòrics. A l'hora de definir el marc de controls, al no tenir un pressupost establert o certs límits reals plantejats per una organització, a nivell teòric podríem haver anat a l'extrem i afegir tots els controls que haguéssim volgut fins a aconseguir un nivell de risc residual de pràcticament 0, cosa que és completament impossible a la vida real.

10.2 Dedicació i cost temporal

La dedicació temporal durant la realització d'aquest treball es pot desglossar dins de les següents fases:

Marc teòric

- Plantejament del treball i temes a tractar: 15 hores
- Recerca d'informació: 60 hores
- Redacció: 30 hores
- Dedicació total al marc teòric: 105 hores

Cas pràctic

- Definició dels escenaris i del cas a estudiar: 15 hores
- Recerca d'informació: 25 hores
- Estudi de la metodologia utilitzada: 5 hores
- Càlculs, valoració de controls i cobertures i anàlisi de riscos: 50 hores
- Elaboració de taules i redacció: 30 hores
- Total cas pràctic: 125 hores

Redacció de la memòria

- Introducció, objectius i resum del treball: 4 hores
- Comparació amb la solució cloud: 4 hores
- Conclusions del treball: 4 hores
- Reunions amb la tutora i correccions: 8 hores
- Format i revisió de la memòria: 10 hores
- Total redacció de la memòria: 30 hores

Dedicació total: 260 hores

10.3 Línies de futur del treball

Com a passos a seguir un cop realitzat el treball, una idea que ens sembla molt interessant tant a mi com a la Laura és fer el mateix exercici que hem fet pel servei de correu corporatiu però aplicat a una organització sencera i a totes les parts que la composen. Tot i que no tindria sentit enfocar-ho com una organització completament on-premise o completament en cloud ja que hi ha molts serveis que només tenen sentit quan s'ofereixen sota un dels dos paradigmes, si que seria interessant analitzar una organització al complert per comprendre el seu funcionament i tenir una visió més general del conjunt de riscos que apareguin. En aquest cas el marc de controls a implementar també seria bastant més extens i tocaria altres dominis com la seguretat física o la part legal en les que no s'ha fet tant d'èmfasi en aquest treball.

No cal dir que una altra via d'estudi a futur és la evolució de totes les tecnologies comentades en els nostres treballs, tant per les capacitats de seguretat clàssiques, que contínuament incorporen noves funcionalitats per adaptar-se a les noves amenaces com per tota la

securització de l'entorn cloud, que tenint en compte la tendència a migrar serveis cap al núvol, segur que presentarà avenços importants durant els propers anys.

10.4 Conclusió

Aquest treball ha sigut un dels projectes que més m'ha motivat durant la meva trajectòria acadèmica, ja que per primer cop he tingut la oportunitat de dur a terme una recerca orientada al camp al que em dedico laboralment i que m'apassiona.

Amb la realització del marc teòric he pogut consolidar alguns coneixements que ja havia adquirit referents a la seguretat i a la gestió de riscos, i també aprendre molts conceptes que o no coneixia o no era conscient de que eren rellevants en aquest camp. La recerca d'informació també ha sigut molt útil per conèixer tendències, noves tecnologies, algunes curiositats i també fonts fiables d'informació sobre seguretat informàtica d'on treure informació en el futur.

També ha sigut molt la realització del cas pràctic ja que un anàlisi de riscos al complert no l'havia fet mai i m'ha servit per veure les diferents fases a seguir i per aprendre a analitzar els resultats obtinguts. El que al principi semblava una tasca molt complexa, amb moltes fases i amb la necessitat d'ajuntar moltes peces, ara sembla més senzill i estructurat i si ho tornés a fer no em trobaria amb tantes dificultats.

Finalment, també m'emporto d'aquest projecte tot el que he après al treballar amb la Laura, durant tots els cops que hem comentat els passos a seguir per realitzar el treball de principi a fi i per anar definint els objectius a assolir. El fet de realitzar dos treballs amb una part en comú ens ha fet desenvolupar una de les habilitats principals que s'intenten potenciar en el màster que estem cursant i és la capacitat de treballar en equip.

11 Bibliografia

ISC2 (2015), Certified Information Systems Security Professional – Official Study Guide (7th Edition). USA.

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

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

John M. Gilligan (2009), 20 Most Important Controls For Continuous Cyber Security Enforcement, https://csrc.nist.gov/CSRC/media/Events/ISPAB-APRIL-2009-MEETING/documents/ispab_jgilligan_april2009.pdf , Consultat al Desembre de 2017

Advisera, 27001 Academy (2017) ¿Qué es la norma ISO 27001? https://advisera.com/-27001academy/es/que-es-iso-27001/, Consultat al Gener de 2018

Heimdal Security (2018), 10+ Critical Corporate Cyber Security Risks – A Data Driven List https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/, Consultat al Gener de 2018

Beckhoff, OSI Model https://infosys.beckhoff.com/english.php?content=../content/1033-/tf6310-_tc3_tcpip/9007199338987915.html&id, Consultat al Febrer de 2018

Institut Obert de Catalunya (2018), Xarxes d'àrea localhttp://ioc.xtec.cat/materials/FP-/Materials/2201_SMX/SMX_2201_M05/web/html/WebContent/u1/a2/continguts.html, Consultat al Febrer de 2018

Ymant (2015), DMZ "zona desmilitaritzada" http://www.ymant.com/dmz-zona-desmilitarizada/, Consultat al Febrer de 2018

Kaspersky Labs (2018), ¿Qué es el phishing? https://securelist.lat/threats/que-es-el-phishing/ , Consultat al Març de 2018

Paloalto Networks (2018), What is a denial of service attack? https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos Consultat al Març de 2018

Paloalto Networks (2018), What is a distributed denial of service attack? https://www.paloaltonetworks.com/cyberpedia/what-is-a-ddos-attack, Consultat al Març de 2018

The Guardian (2016), DDoS attack that disrupted internet was largest of its kind in history, experts say https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet, Consultat al Març de 2018

Steve Friedl, Unixwiz (2008), An Illustrated Guide to the Kaminsky DNS Vulnerability, http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html, Consultat al Març de 2018

Paloalto Networks (2018), APT Prevention, https://www.paloaltonetworks.com/-features/apt-prevention, Consultat al Març de 2018

Antoine Vigneron (2014), Cybersecurity: Issues and ISACA's response, https://www.slideshare.net/AntoineVigneron/symposium-afai-cybersecurity-csx-isaca, Consultat al Març de 2018

Panda Security (2018), Amenazas Persistentes Avanzadas, https://www.pandasecurity.com/spain/mediacenter/consejos/amenazas-persistentes-avanzadas/, Consultat al Març de 2018

Pietr Arntz, Malwarebytes (2016), https://blog.malwarebytes.com/cybercrime/malware/2016/07/explained-advanced-persistent-threat-apt/, Consultat al Març de 2018

Scientific American (1998), When did the term 'computer virus' arise, https://www.scientificamerican.com/article/when-did-the-term-compute/, consultat l'Abril de 2018

Kaspersky Labs (2017), What is a trojan virus?, https://www.kaspersky.com/resource-center/threats/trojans, Consultat a l'Abril de 2018

Cisco (2018), What Is the Difference: Viruses, Worms, Trojans, and Bots? https://www.cisco.com/c/en/us/about/security-center/virus-differences.html, Consultat a l'Abril de 2018

Pietr Arntz, Malwarebytes (2018), Explained: SQL Injection, https://blog.malwarebytes.com/security-world/business-security-world/2018/03/explained-sql-injection/, Consultat a l'Abril de 2018

Rapid 7 (2018), SQL Injection Attacks (SQLi), https://www.rapid7.com/fundamentals/sql-injection-attacks/, Consultat a l'Abril de 2018

AENOR (2018), ISO 27001, https://www.aenor.es/aenor/certificacion/seguridad/-seguridad_27001.asp#.WtMnUIhubD4, Consultat al Febrer de 2018

Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh (2008), Technical Guide to Information Security Testing and Assessment, https://csrc.nist.gov/publications/detail/sp/800-115/final, Consultat al Febrer de 2018

APDCAT (2018), Principales novedades del RGPD http://apdcat.gencat.cat/es/documentacio/RGPD/novetats/, Consultat al Febrer de 2018

Margaret Rouse (2015), Los 12 requisitos PCI DSS), https://searchdatacenter.techtarget.com/es/definicion/Los-12-requisitos-PCI-DSS, Consultat al Febrer de 2018

CISCO (2018), What is a Firewall? https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html, Consultat al Juny de 2018

ABAST (2018), Next Generation Firewalls, http://www.abast.es/ca/ciberseguretat/solucions-de-seguretat-ti/next-generation-firewalls-ngfw/, Consultat al Juny de 2018

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

Panda Security (2018), ¿Qué es un ransomware?, https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/, Consultat al Maig de 2018

Norton (2018), 7 tips to prevent ransomware, https://us.norton.com/internetsecurity-malware-7-tips-to-prevent-ransomware.html, Consultat al Maig de 2018

Wendy Zamora, MalwareBytes (2015), https://blog.malwarebytes.com/101/2015/09/-whats-the-difference-between-antivirus-and-anti-malware/, Consultat al Juny de 2018

Curtis Cade, OPSWAT (2015), Understanding Heuristic-based Scanning vs. Sandboxing, https://www.opswat.com/blog/understanding-heuristic-based-scanning-vs-sandboxing, Consultat al Juny de 2018

SANS Institute (2006), A Practical Application of SIM/SEM/SIEM Automating Threat Identification, https://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781, Consultat al Juny de 2018

Deloitte (2018), MASTERCLASS: Ciberseguridad SIEM, https://www.youtube.com/watch?v=uhxhJJJSQXM&t=4s

CISCO (2008), How Virtual Private Networks Work, https://www.cisco.com/c/en/us/supp-ort/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html, Consultat al Juny de 2018

HKSAR (2008), VPN Security, https://www.infosec.gov.hk/english/technical/files/vpn.pdf, Consultat al Juny de 2018

Microsoft (2014), How VPN Works, https://technet.microsoft.com/pt-pt/library/cc779919(v=ws.10).aspx, Consultat al Juny de 2018

Symantec (2018), Symantec Data Loss Prevention, https://www.symantec.com/products/data-loss-prevention, Consultat al Juny de 2018

Symantec (2015), ¿Por qué un DLP?... By Symantec, 22Sep2015 https://www.youtube.com/watch?v=r4vzGR-Ct9k&t=2132s

Cyberark (2018), Privileged Session Managerhttps://www.cyberark.com/-products/privileged-account-security-solution/privileged-session-manager/, Consultat al Juny de 2018

Wallyx (2018), Privileged Access Management Features, http://blog.wallix.com-/privileged-access-management-features-pam-features, Consultat al Juny de 2018

David Bisson (2018), Cloud vs. On-Premises: Understanding the Security Differences, https://www.tripwire.com/state-of-security/security-data-protection/cloud/cloud-vs-premises-security/, Consultat al Juny de 2018

Gartner (2018), Gartner Forecasts Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018, https://www.gartner.com/newsroom/id/3871416, Consultat al Juny de 2018

Grant Leonard (2018), IDS, IPS and UTM - What's the Difference?, https://www.alienvault.com/blogs/security-essentials/ids-ips-and-utm-whats-the-difference, Consultat al Juny de 2018

Juniper (2018), What is IDS and IPS?, https://www.juniper.net/us/en/products-services/what-is/ids-ips/, Consultat al Juny de 2018

12. Annex

A continuació s'adjunta el document excel que conté l'anàlisi de riscos realitzat:

Anàlisi de riscos -
Correu corporatiu On

S'adjunta també el treball de la Laura Abellanet, companya del Màster en enginyeria de telecomunicacions i que complementa a aquest treball:

TFM Laura Abellanet.
Anàlisi de la cibersegu