Auditoria interna de seguretat informàtica aplicable a qualsevol organització

Maria Teresa Muñoz Siles

Professor Consultor: José Manuel Castillo Pedrosa

Professorat Responsable: David Bañeres Besora

Montse Serra Vizern

Grau d'Enginyeria Informàtica

Àrea TFG: Administració de xarxes i sistemes operatius

Dedico aquest treball als meus éssers estimats, pel seu suport constant per encoratjar-me a continuar aquest llarg camí, tant de creixement personal com intel·lectual, i especialment, aquells que ja no hi són aquí però que sempre portaré al meu cor.

Al meu professor d'aquest treball, Manuel Castillo Pedrosa, i als meus tutors i professors pels seus ànims i suport al llarg de la meva trajectòria a la universitat.

A tots ells, el meu sincer agraïment per la seva paciència, esforç i consideració.

Títol del treball:	Auditoria interna de seguretat informàtica aplicable a qualsevol organització
Nom de l'autor:	*Mª Teresa Muñoz Siles*
Nom del consultor:	*Manuel Castillo Pedrosa*
Data de lliurament (mm/aaaa):	*23/12/2022*
Àrea del Treball Final:	*Administració de xarxes i sistemes operatius*
Titulació:	*Grau d'Enginyeria Informàtica*

Resum del Treball (màxim 250 paraules):

Actualment qualsevol organització manipula tant sistemes informàtics com informació per tal de desenvolupar les seves activitats de forma eficient i eficaç, aprofitant els constants avenços de les tecnologies de la comunicació i la informació.
Però això comporta uns riscos davant les amenaces a les que s'exposen aquests actius diàriament, la seguretat dels quals es pot veure compromesa pel continu creixement d'intrusions i ciberatacs, tant interns com externs.

Per evitar-los o reduir-los al màxim, és molt recomanable que les organitzacions es conscienciïn de la necessitat d'efectuar auditories internes de forma periòdica ja que les ajudaran a descobrir vulnerabilitats i males pràctiques, que han passat desapercebudes però que constitueixen una porta oberta a atacants, i establir així el punt de partida per planificar les mesures conduents a la seva correcció.

El model d'auditoria interna que s'exposa es basa en les normes estàndards ISO 27001:2017 i norma ISO/IEC 27002:202. Com a avantatge, presenta la seva adaptació a qualsevol tipus d'activitat empresarial i serà de molta utilitat per dificultar les accions d'intrusos, així com per sensibilitzar a tots els integrants de l'organització de la importància de desenvolupar unes bones pràctiques per enfortir la seguretat informàtica.

Tot això, en conjunt, permetrà tant prevenir la destrucció o modificació de la informació i garantir la continuïtat del negoci, com evitar problemes legals deguts a la pèrdua de confidencialitat de les dades, entre d'altres incidències, i al mateix temps, beneficiarà la competitivitat i la imatge de l'organització a l'oferir un producte o servei de major qualitat i fiabilitat.

Abstract (in English, 250 words or less):

Nowadays, any organization operates both computer systems and information in order to develop its activities efficiently and effectively, taking advantage of the constant advances in communication and information technologies.

But this means risks in the face of the threats to which these assets are exposed on daily, the security of which can be compromised by the continuous growth of intrusions and cyber attacks, both internal and external.

To avoid them or reduce them as much as possible, it's highly recommended that organizations become aware of the need to carry out internal audits periodically as they will help them to discover vulnerabilities and bad practices, which have gone unnoticed although they constitute a open door to attackers, and in this way establish the starting point for planning the measures leading to its correction.

The internal audit model presented is based on the ISO 27001:2017 and ISO/IEC 27002:202 standard rules. As an advantage, it presents its adaptation to any type of business activity and will be very useful to difficult the actions of intruders, as well as to sensitize all members of the organization to the importance of developing good practices to strengthen IT security.

All of this, altogether, will both prevent the destruction or the modification of information and guarantee business continuity, as well as avoid legal problems due to the loss of data confidentiality, among other incidents, and at the same time, it will benefit the competitiveness and the image of the organization by offering a product or service of better quality and reliability.

Paraules clau (entre 4 i 8):

Auditoria interna, Seguretat informàtica, norma ISO/IEC 27001:2017, norma ISO/IEC 27002:2022, confidencialitat, vulnerabilitats, integritat, disponibilitat de la informació.

Índex

Índex de Taules

Índex de Figures

Annexos

1. Introducció

Actualment, les organitzacions treballen de forma molt intensiva amb equips informàtics i de telecomunicacions, independentment del sector que ocupin. Qualsevol procés empresarial integra el seu ús, des del control d'accés a un edifici fins a l'enviament de documentació amb dades sensibles. Aquests i d'altres actius informàtics es troben exposats a una sèrie de riscos i amenaces molt diversos, com poden ser: accessos no autoritzats, desastres naturals, avaries en els servidors, atacs de virus, errors humans,... Tots ells es poden donar de forma aïllada o combinats, però sigui com sigui, poden comprometre seriosament la seguretat informàtica dels sistemes, i de retruc, afectar molt negativament a l'activitat empresarial.

Així, cal destacar que amb la implementació creixent de les aplicacions web, tal com va publicar l'INCIBE (Instituto Nacional de Ciberseguridad) al seu article *Top 10 vulnerabilidades web de 2021*[1], s'han de posar en marxa les mesures de seguretat adients per evitar que les seves vulnerabilitats puguin ser aprofitades pels ciberdelinqüents, amb els conseqüents impactes que se'n deriven:

Vulnerabilitat	***Impacte***
Pèrdua del control d'accés	Accés a informació no autoritzada per divulgar-la sense permís Accés al sistema amb privilegis d'usuari o administrador
Errors criptogràfics	Les dades confidencials o qualsevol altra informació queda disponible a persones no autoritzades
Injecció de dades infectades o Disseny insegur de l'aplicació	Divulgació, modificació o pèrdua de la integritat de la informació Control sobre els servidors
Configuració defectuosa de la seguretat	Accesos no autoritzats
Components obsolets o vulnerables	La seva explotació pot originar grans bretxes de seguretat
Errors d'identificació i autenticació	Accés a credencials administratives o d'empleats
Errors en el programari i la integritat de les dades	Introducció de codi no autoritzat o indesitjat
Errors en el registre i la supervisió de la seguretat	S'ignora la possible presència d'accessos no autoritzats o possibles accions de ciberdelinqüents al sistema

[1] Top 10 vulnerabilidades web de 2021 [en línia]. [Consulta: 9 d'octubre de 2022]. <https://www.incibe.es/protege-tu-empresa/blog/top-10-vulnerabilidades-web-2021>

Falsificació de sol·licitud del costat del servidor	Robatori d'informació confidencial Accés als sistemes de l'organització

Taula 1. Top 10 vulnerabilidades web de 2021

Tot i que no és possible eliminar al 100% aquestes situacions, dins de l'àmbit de la seguretat informàtica es pretén controlar aquest risc, garantir que qualsevol recurs del sistema d'informació s'utilitzi en la forma en què es va decidir i que el seu accés només sigui permés a aquell que estigui autoritzat. La finalitat és aconseguir que els processos siguin més eficients i segurs, minimitzant al màxim els efectes devastadors que es poden originar com a conseqüència d'aquests incidents: manca de confidencialitat de les dades, indisponibilitat de la informació, pèrdua de la integritat de les dades,... inclús pèrdua de la credibilitat de l'organització.

Per això, i per tal de prevenir o reduir els danys que aquests podrien ocasionar, es fa molt aconsellable detectar-los amb suficient antelació per mitjà de l'ajut d'eines com poden ser les auditories internes. Aquestes revisions permeten, entre d'altres aspectes, analitzar els sistemes i recursos informàtics, estudiar com es gestionen i verificar que compleixen amb la normativa, a fi de detectar deficiències i establir les mesures per corregir-les. Alhora, el seu desenvolupament i execució periòdica es converteix en un procés de millora contínua molt beneficiós per a l'organització pel que deuria d'integrar-se al llarg del cicle de vida dels sistemes informàtics, tal com s'exposarà més endavant.

1.1. Context i justificació del treball

Aquest treball gira entorn a les auditories, però no tracta de les externes, que són més conegudes pel fet, principalment, de permetre l'obtenció d'una certificació si el procés d'avaluació ha finalitzat amb éxit. En concret, es treballarà un model d'**auditoria interna de seguretat informàtica** de forma que serveixi com a guia per poder desenvolupar-la i que resulti **apta per a qualsevol tipus d'organització**, independentment del seu tamany, de la seva activitat o de si aquesta és privada o pública.

Aquesta auditoria, realitzada de manera voluntària, es converteix en una eina de gran ajuda per garantir una major seguretat dels sistemes informàtics, elements sense els quals seria impossible realitzar i controlar totes les activitats i processos crítics que desenvolupen les organitzacions. La seva necessitat es fa cada vegada més patent, atesa la diversitat i el volum creixent de les operacions que s'han de realitzar a diari i que consumeixen grans quantitats d'informació, ja que en la mesura del possible, cal evitar que els processos quedin aturats com a conseqüència d'un incident que afecti als seus actius d'informació.

Per tant, l'auditoria interna no es desenvoluparà dins d'una empresa real, ja que el que es pretén és que pugui resultar útil per les organitzacions de qualsevol sector interessades en conèixer el

seu estat a nivell de seguretat informàtica. D'aquesta manera, es poden dissenyar posteriorment les estratègies que garanteixin el seu bon funcionament davant l'aparició de possibles atacs o d'altres factors que puguin malmetre els seus actius d'informació o la pròpia informació (per robatori, destrucció, eliminació accidental, enginyeria social,...)

Tal com es mostra al següent gràfic, les empreses de qualsevol sector es poden veure afectades per algun incident de seguretat informàtic. En alguns casos, hi ha sectors on es sobrepassen els dos incidents per any (Assegurances, Banca, Telecomunicacions, Indústria), fet que evidencia la importància de realitzar periòdicament auditories internes:

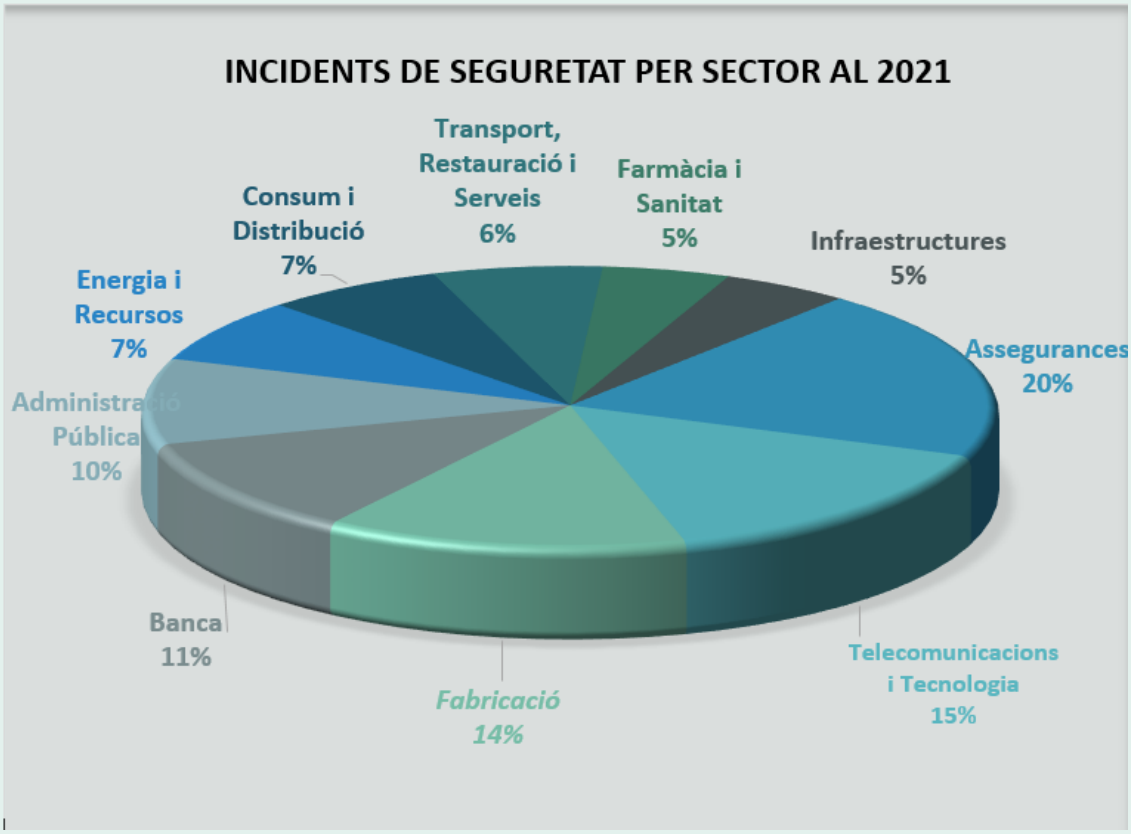


Figura 1. Gràfic elaborat a partir de 'El estado de la ciberseguridad en España" de Deloitte.
Informació accessible des de: *https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html*

A l'hora d'auditar la seguretat informàtica dels actius, cal tenir en compte que aquests són molt diversos i que no es limiten únicament al maquinari ubicat a les instal·lacions empresarials. Segons la metodologia *Magerit*, els actius que protegeix la seguretat informàtica es poden dividir en diferents grups segons la seva naturalesa. D'aquesta manera, podríem obtenir la següent classificació:

Figura 2. Classificació dels actius segons la metodologia Magerit

1.2. Objectius del treball

L'objectiu principal d'aquest treball és la realització d'un **model d'auditoria interna de seguretat informàtica** que sigui compatible a qualsevol organització.

En funció dels resultats obtinguts, aquesta podrà implementar un **pla de millora per tal de detectar possibles riscos, prevenir-los o reduir-los** a nivells mínims a través de mesures correctores i preventives.

Tot i així, també cal exposar d'altres objectius que se'n deriven d'aquesta auditoria interna i que, en conjunt, serviran per prendre mesures conduents a la millora de la seguretat informàtica:

- ✓ Comprovar el correcte compliment dels procediments, normes, polítiques i controls interns.
- ✓ Analitzar l'eficiència, confiabilitat i rendiment operacional dels sistemes informàtics.
- ✓ Estudiar les causes de danys anteriors per planificar la seguretat en el futur.
- ✓ Elaborar plans més efectius de recuperació després d'un desastre que permetin restaurar el sistema de la forma més adequada per reduïr pèrdues, i plans preventius, per evitar els desastres o les amenaces cap la informació o els actius que la tracten en la mesura del possible.
- ✓ Reduir les pèrdues o l'impacte ocassionats per un succés intrusiu.
- ✓ Protegir la confidencialitat, integritat i disponibilitat de la informació.
- ✓ Garantir que es fa un bon ús dels sistemes informàtics.
- ✓ Millorar la qualitat de la informació (evitant la duplicitat, garantint la integritat,…)

1.3. Enfocament i mètode seguit

L'auditoria interna es planteja amb un abast que inclogui a tota l'organització, és a dir, totes aquelles àrees, departaments, processos i activitats en les que l'ús de sistemes informàtics és present.

Tot i que per la seva metodologia, també s'adapta de forma molt flexible a un únic departament o a uns processos concrets, si per les dimensions de l'organització es recomanés reduir el seu abast. En aquest cas, es podria desenvolupar en diferents fases fins completar totes les àrees de l'organització.

En concret, s'enfoca a tots aquells elements que afecten a la seguretat informàtica:

Seguretat física

-Maquinari

-Manipulació dels equips

-Entorn i instal·lacions

Seguretat lògica

-Sistemes operatius

-Aplicacions

-Informació

Seguretat de la xarxa

-Xarxes de comunicació

Figura 3. Elements afectats per la seguretat informàtica inclosos dins l'auditoria interna

Per tant, es tracta d'una activitat que afecta als processos, recursos i sistemes d'informació, però també al personal intern de l'organització i als tercers que interaccionen amb l'activitat d'aquesta (proveïdors, clients,...)

Així mateix, l'auditoria interna es basarà en normes estàndards com ho són les normes ISO/IEC 27001:2017[2] i ISO/IEC 27002:2022[3], que són de compliment voluntari, però que són l'eix central donada la seva importància al definir el camí a seguir amb l'objectiu de que els sistemes i recursos de l'organització siguin més segurs i confiables.

Tot això, sense oblidar que també cal atenir-se als aspectes legals, sobretot pel que fa a la legislació de protecció de dades vigent ja que aquesta és d'obligat compliment.

[2] Guía de iniciación a actividad profesional. Implantación de sistemas de gestión de la seguridad (SGSI) según la norma ISO 27001 [en línia]. [Consulta: 17 d'octubre de 2022]. https://www.coit.es/informes/implantacion-de-sistemas-de-gestion-de-la-seguridad-de-la-informacion-sgsi-segun-la-norma

[3] Patiño, S., Caicedo, A., & Guaña, E. R. (2019). Modelo de evaluación del dominio control de acceso de la norma ISO 27002 aplicado al proceso de gestión de bases de datos. Revista Ibérica De Sistemas e Tecnologias De Informação, 230-241 [en línia]. [Consulta: 1 d'octubre de 2022]. <https://www.proquest.com/scholarly-journals/modelo-de-evaluación-del-dominio-control-acceso/docview/2317841707/se-2

1.4. Planificació del treball

S'inclouen els cronogrames en els que es desglossen per dates les diverses activitats de l'auditoria que es desenvoluparan dins de cadascuna de les PAC:

- Per a la PAC 2 les tasques són de caire més preparatori de cara a l'auditoria (veure *Annex I*). En línies generals, es tracten les activitats prèvies per a la seva planificació, incloent els recursos i documents necessaris. Tot això, atenint-se a les normes aplicables i subratllant la importància de dur-la a terme donats els beneficis que suposa per a l'organització.

- Durant la PAC 3 es realitzaran la resta d'activitats de l'auditoria, conduents al seu desenvolupament (disseny d'entrevistes, proves tècniques,...), que s'executen fins a la seva finalització i que serviran per a que l'auditor proposi totes aquelles mesures i recomanacions per protegir els actius d'informació. D'aquesta manera, s'arriba a la creació de l'informe final de l'auditor intern. A més, dins del mateix cronograma (veure *Annex II*), s'han inclòs les darreres tasques corresponents a l'entrega final del treball del TFG.

2. Les auditories informàtiques i la seva tipologia

L'auditoria informàtica és un procés sistemàtic i independent en el que es duen a terme diverses activitats d'avaluació de la gestió dels sistemes informàtics, que prenen com a referència normes nacionals i internacionals[4].

Les seves fases, que s'han d'executar de forma seqüencial i ordenada, han de quedar degudament documentades i han de complir amb el cicle de qualitat:

Figura 4. Fases d'una auditoria informàtica

[4] ISO27000 [en línia]. [Consulta: 30 de setembre de 2022]. <http://www.iso.org>

Entre les diverses activitats que cal **executar** durant una auditoria es poden trobar: la recol·lecció d'informació en relació a procediments, arxius i d'altres actius; la revisió de l'entorn on es desenvolupa l'activitat; l'avaluació de les evidències obtingudes durant la seva execució,...

Totes elles impliquen la seva **planificació** i coordinació prèvia, l'establiment d'un calendari, el consens amb la Direcció per determinar el seu abast,...

En conjunt, les activitats tindran com a finalitat **avaluar** si els sistemes informàtics poden donar una resposta efectiva davant de qualsevol eventualitat (un atac informàtic de denegació de servei o DoS, una pèrdua accidental d'informació,...)

És per això que es pot considerar com un element de control a les organitzacions que s'ha d'incloure dins del cicle de vida dels sistemes informàtics, a fi d'analitzar la seva eficiència i eficàcia, però que no parteix de la idea que existeixin problemes de seguretat previs.

Finalment, si es localitzen vulnerabilitats, l'organització haurà d'**actuar** aplicant les recomanacions i les mesures per corregir-les, a partir de les quals poden desenvolupar o millorar les polítiques de seguretat per poder prevenir o afrontar els atacs en cas que es produeixin al mateix temps que adapten les seves capacitats per preparar-se davant de situacions de risc.

Però tots els processos i activitats que es desenvolupen al llarg de l'auditoria interna tindran sentit sempre i quan s'efectuï el seguiment de les mesures correctores implantades a fi de verificar que s'obté el resultat esperat.

Segons la seva tipologia, cal distingir les següents auditories[5]:

[5] Auditoría interna y los riesgos de la ciberseguridad. [10 d'octubre de 2022]. [Consulta:]. <https://www.bing.com/ck/a?!&&p=26ae1e58b7ca88d4JmltdHM9MTY2NzYwNjQwMCZpZ3VpZD0zMjdlMDNiNy0xMDJjLTZlNmEtMGU2NC0xMWU0MTE2NTZmZWUmaW5zaWQ9NTE3OQ&ptn=3&hsh=3&fclid=327e03b7-102c-6e6a-0e64-11e411656fee&psq=Auditor%c3%ada+interna+y+los+riesgos+de+la+ciberseguridad.+KPMG&u=a1aHR0cHM6Ly9hc3NldHMua3BtZy9jb250ZW50L2RhbS9rcG1nL2FyL3BkZi8yMDIwL2F1ZGl0b3JpYS1pbnRlcm5hLXktbG9zLXJpZXNnb3MtZGUtY2liZXJzZWd1cmlkYWQucGRm&ntb=1>

Figura 5. Tipologies d'auditories informàtiques

Per tant, l'auditoria, ja sigui externa o interna, en funció dels resultats obtinguts ens permetrà escollir aquelles mesures més adients per corregir les deficiències detectades i millorar la seguretat:

- **Organitzatives:** a través de mesures orientades als empleats, com pot ser l'establiment de procediments per donar d'alta o baixa als usuaris, o accions formatives per millorar les seves competències en seguretat.

- **Tècniques:** mesures que fan servir la tecnologia, com són l'ús de tallafocs, maquinari redundant, monitorització de la xarxa,...

- **Físiques:** mesures de protecció, com poden ser el control dels accessos per poder accedir a les dependències de l'organització o guardar els suports que contenen informació en un lloc segur.

2.1. Beneficis de l'auditoria interna

Les auditories proporcionen molts avantatges a les organitzacions, però en el cas específic de l'auditoria interna es poden enumerar els següents beneficis, sempre i quan aquest procés s'executi de forma adequada:

- elaborar **un informe d'auditoria final amb les recomanacions per establir un pla de millora de la seguretat** de les infrastructures de les tecnologies de la informació i de la comunicació que es fan servir a una organització, al poder detectar possibles mancances o defectes en els sistemes. El fet de conèixer-los permet aplicar les tasques o mesures correctores necessàries per resoldre'ls definitivament o establir millores en el Pla de Seguretat de la Informació.
  Cal tenir en compte que a les empreses, un dels actius intangibles que presenta una major criticitat és la informació, ja que és fonamental per poder mantenir la continuïtat de la seva activitat amb normalitat.

- **minimitzar l'impacte financer, legal i operatiu** que pot originar una protecció insuficient de la informació i els actius amb què es crea, processa, es guarda o es transmet. Així, per exemple, pot prevenir les sancions legals degudes a la pèrdua o a incidents amb la informació.

- **proporcionar una cultura empresarial amb una major conscienciació** de la importància d'incloure accions conduents a preservar la seguretat dels sistemes d'informació, com és el cas d'aquesta auditoria interna. Tot i no ser un procés obligatori per les organitzacions, degut a que compleix una funció primordial dins de l'àmbit de la seguretat informàtica, no ha de ser menystingut.

- en relació al punt anterior, es converteix en una eina que **pot facilitar en gran mesura el camí cap a la certificació d'una empresa** al finalitzar un procés d'una auditoria externa amb éxit, si prèviament, l'auditoria interna s'ha executat convenientment amb una aplicació correcta de les recomanacions de millora donades. Una vegada obtinguda la certificació, aquesta té una validesa de 3 anys, després dels quals es realitza la seva renovació i es realitzen auditories de seguiment cada any.

- **complir amb la normativa de protecció de dades tant personals com de la pròpia organització**, al protegir les dades que els actius d'informació poden contenir referent a clients, treballadors de la pròpia organització, proveïdors,...
  Tal com descriu l'INCIBE a la seva guia 'Protección de la información'[6], existeixen diferents categories d'informació, cadascuna de les quals requereix d'un tractament diferent:

[6] Protección de la información [en línia]. [Consulta: 15 d'octubre de 2022]. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

CATEGORIA	DESCRIPCIÓ	TRACTAMENT
Confidencial	La més sensible per a l'organització Restringida a la Direcció i determinats empleats Inclou dades personals sotmesos al règim jurídic especial	Exigeix control d'accés S'ha d'identificar convenientment Atenció a la legislació aplicable Fora de l'empresa cal xifrar-la
Interna	Informació d'abast a tots els empleats Directori personal, intranet corporativa	Etiquetatge de la informació Difusió prohibida a tercers, només permesa sota autorització de la Direcció
Pública	Sense restricció Informació comercial	No requereix tractament especial

Taula 2. Classificació de la informació basada en la guia de l'INCIBE 'Protección de la información'

- maximitzar la **productivitat i eficiència dels sistemes informàtics** al poder conèixer amb més precisió quines són les mancances o deficiències en seguretat, redistribuïnt les inversions en aquelles àrees on siguin necessàries de la forma més adequada possible perquè no suposin un excès o una mancança.

- facilitar a la Direcció **la presa de decisions** al proporcionar una informació de major qualitat, exacta, actualitzada i completa.

- planificar les activitats incloses dins del **desenvolupament d'un procés d'auditoria interna** conduents a detectar possibles vulnerabilitats (defectes de les aplicacions, antivirus desfasats,...). També permet preveure amenaces provinents d'atacants o d'altres factors que poden aprofitar-se d'aquestes debilitats, és a dir, les causes potencials que poden originar un incident indesitjat. D'aquesta manera, es pot mesurar d'una forma objectiva quina és la capacitat del sistema per garantir les següents dimensions de la seguretat de la informació (disponibilitat, confidencialitat i integritat), a les quals podem afegir altres característiques per proporcionar majors garanties que la informació emmagatzemada i processada és de qualitat i útil per al negoci:

- **disponibilitat:** al proporcionar una major garantia d'accés als recursos i sistemes que contenen la informació en el moment en què l'usuari la requereixi.
- **confidencialitat:** a l'accedir a la informació només aquelles persones que hi estiguin autoritzades.
- **integritat:** al disposar d'informació vàlida, correcta i lliure d'errors, que no ha estat alterada o modificada.
- **autenticitat:** al comprovar que l'usuari que vol accedir a un sistema és qui diu ser, per mitjà d'alguna cosa que aquest ja poseeix, és o coneix, i que en el moment de donar-se d'alta es va assignar a la seva identitat (per exemple: empremtes digitals, PIN, credencials,...)
- **traçabilitat:** a l'enregistrar un històric dels accessos i les modificacions de les dades al llarg de tots els processos que es realitzen a través dels seus actius d'informació. D'aquesta manera, permet auditar quins usuaris han modificat o accedit a una determinada informació.

Figura 6. Característiques de la informació útil i de qualitat

- **auditabilitat**: a l'enregistrar els successos d'un sistema per poder-los controlar posteriorment.
- **protecció a la duplicació:** s'evita que una petició realitzada per un usuari es reprodueixi múltiples vegades a l'assegurar que la transacció es realitza una única vegada, si no es demana el contrari.
- **no repudi:** s'evita que aquell que ha enviat o rebut una informació no pugui negar que va ser així.
- **legalitat:** el tractament de la informació també implica assegurar el compliment d'aquelles lleis i normativa a la que es trobi subjecta l'organització.
- **confiabilitat de la informació**: no tindria sentit treballar amb una informació inadequada per poder prendre decisions o desenvolupar les operacions necessàries per al bon funcionament empresarial.

- **millorar la imatge de l'organització cap a l'exterior**, al percebre els seus usuaris i proveïdors que els seus sistemes són segurs, confiables i ofereixen un servei de qualitat. Per tant, es millora el servei i l'atenció als clients de l'organització.

En definitiva, la revisió de la seguretat informàtica per mitjà d'auditories internes estalviarà a l'organització de moltes conseqüències negatives, que segons la seva gravetat fins i tot podrien acabar, en el pitjor dels casos, amb la seva desaparició. D'aquestes, s'hi podrien esmentar les següents, que malhauradament no acostumen a produir-se per separat, sinó que l'existència d'una d'elles provoca l'aparició d'altres:

☹ Pèrdua d'integritat o destrucció de la informació
☹ Interrupció del servei
☹ Ineficiència dels processos
☹ Robatori d'informació o de recursos
☹ Desaparició d'informació o amb presència d'errors
☹ Pèrdues econòmiques directes
☹ Desavantatge competitiu per fuga d'informació
☹ Pèrdues de la producció
☹ Marxa de clients
☹ Entrada de virus i correu indesitjat (*spam*)
☹ Imatge negativa i pèrdua de credibilitat
☹ Demandes legals i importants sancions

Taula 3. Conseqüències negatives evitables amb una auditoria interna

3. Requisits legals

3.1. Normes ISO aplicades a l'auditoria interna

Quant a normativa aplicable a l'auditoria, aquesta es basarà en els següents estàndards de seguretat existents que pertanyen a la família de normes ISO 27000 que tracten sobre les tècniques de seguretat i les tecnologies de la informació:

- **Norma ISO/IEC 27001:2017**

  És la norma principal de la sèrie 27000 i especifica els requeriments del Sistema de Gestió de Seguretat de la Informació (SGSI), sigui quin sigui el format en el que aquesta es trobi.

  Aquesta norma incideix sobre tot en aspectes com la **disponibilitat, confidencialitat i integritat** de la informació i dels sistemes encarregats de tractar-la, segons les necessitats de l'organització, aplicant els requeriments conduents a l'operació, implementació, revisió i millora d'aquests sistemes, adaptats a les necessitats de cada organització.

  En aquesta norma, es recullen quins són els documents mínims que han de formar el sistema, els components d'aquest i els registres que donin evidència del seu bon funcionament.

  Com a avantatge d'aquesta norma cal tenir present que pot aplicar-se **a qualsevol organització**, sigui quin sigui el seu tamany o el sector de negoci al que es dediqui.

  Com que és una norma enfocada cap a la **millora contínua**, es pot compatibilitzar amb la resta de sistemes de gestió que ja es troben a l'organització.

  Així mateix, és la norma que també es segueix per a la **certificació** per una tercera part independent del Sistema de Gestió de la Seguretat de la Informació (SGSI) d'aquelles organitzacions interessades.

  De fet, la norma estableix que per dur a terme la implantació d'un SGSI a l'organització fins assolir la certificació en ISO-27001, cal seguir un procés dins del qual s'inclou l'auditoria interna com una de les etapes prèvies a realitzar:

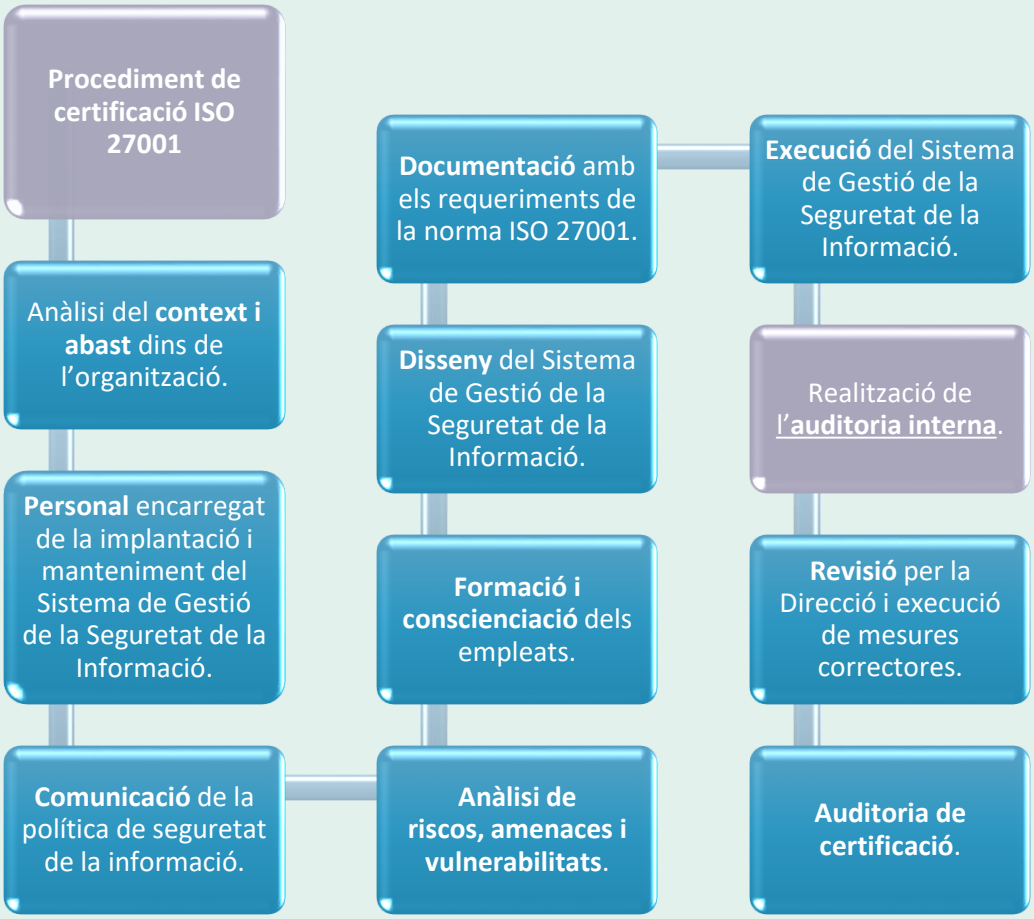


Figura 7. Fases d'implantació d'un SGSI per assolir la certificació en ISO-27001

- **Norma ISO/IEC 27002:2022**

  Tot i que és aplicable a contextos no informàtics, ofereix les **millors pràctiques recomanades en la seguretat del sistemes d'informació** de les organitzacions a partir d'una sèrie d'objectius de control i controls recomanables per gestionar el risc analitzat, pel que també es pot utilitzar com una guia per assolir-la.
  Així, els 93 controls d'aquesta norma s'agruparien sota les següents 4 clàusules:

  - 37 Controls Organitzatius
  - 8 Controls de Persones
  - 14 Controls Físics
  - 34 Controls Tecnològics

Un dels punts a destacar d'aquesta norma és la importància que es donen al **compromís per part de la Direcció** i a la **implicació del personal** en el seu compliment, ja que en cas contrari, suposaria un fracàs la seva implementació. Per això, la norma també inclou les auditories com una eina per conèixer si realment es compleix.

La norma ISO/IEC 27002:2022 inclou 11 nous controls[7]:

Intel·ligència d'amenaces	Cal obtenir informació referent a les amenaces, tant de caràcter estratègic com tàctic i operacional.
Seguretat de la informació en l'ús de serveis en el núvol	Cal desenvolupar procediments per gestionar els serveis al núvol.
Preparació de les TIC per a la continuïtat de negoci	Cal diferenciar la continuïtat del negoci de la continuïtat TIC i per això, s'han de gestionar de manera diferent.
Monitorització de la seguretat física	S'ha d'incorporar un control dels accessos físics no autoritzats.
Gestió de la configuració	La configuració dels actius ha de garantir el seu correcte funcionament, així com controlar que no es canviï sense autorització.
Esborrat d'informació	Garantir el compliment dels terminis de conservació de la informació
Prevenció de fuita de dades	Ús d'eines DLP per detectar la fuita de dades.

[7] Nueva ISO/IEC 27002:2022: cambios con respecto a la versión de 2013 [en línia]. [Consulta: 2 d'octubre de 2022]. <https://www.isotools.org/2022/07/22/nueva-iso-iec-270022022-cambios-con-respecto-a-la-version-de-2013/#:~:text=La%20respuesta%20a%20incidentes%20de%20seguridad%20de%20ISO%2FIEC,informaci%C3%B3n.%20Algunos%20de%20los%20cambios%20m%C3%A1s%20relevantes%20son%3A>

Filtratge web	Reduir el risc d'accés a continguts maliciosos mitjançant restriccions en la navegació dels usuaris.
Control de codificació segura	Requereix tant una política com metodologies de desenvolupament segur.
Monitorització d'activitats	Ús de sistemes SIEM per detectar possibles amenaces.
Emmascarament de dades	Protegir la seva informació i evitar la seva difusió no autoritzada.

Taula 4. Controls de la norma ISO/IEC 27002:2022

A diferència de l'anterior norma, **no és certificable**.

Les principals àrees sobre les que actua aquesta norma s'exposen tot seguit:

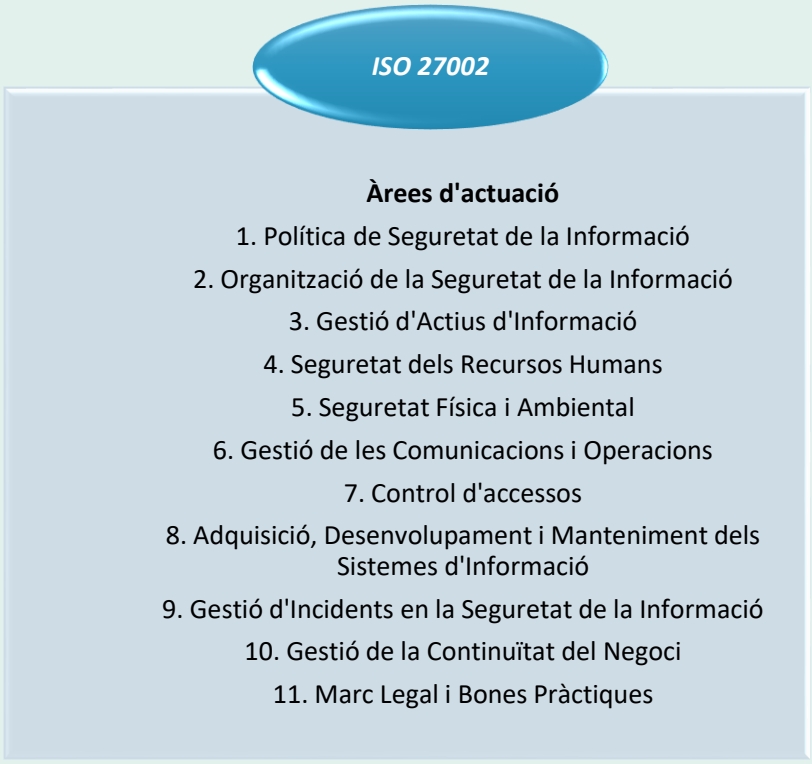


Figura 8. Àrees sobre les que actua la norma ISO 27002

Aquestes normes són de compliment voluntari, però el seu seguiment per part de les empreses resulta clau per millorar la seguretat i la qualitat dels serveis i els productes que desenvolupa.

A més, les mesures encaminades a garantir la seguretat s'han de planificar de forma proporcional a la criticitat dels actius i la informació que s'han de protegir. Això, en un entorn tecnològic en constant canvi, significa que **l'organització haurà d'adaptar-se a les normes i legislació vigents** en consonància amb les noves necessitats en seguretat informàtica que vagin sorgint.

Cal afegir que, en relació a la normativa i la legislació abans esmentada, generalment, les organitzacions també compten amb **normativa interna** que incideix en els recursos i la informació que tracten els usuaris, com pot ser aquella que fa referència a:

- Polítiques de contrasenyes i xifrat d'equips mòbils (portàtils, telèfons intel·ligents,…)
- Accés a pàgines web o xarxes socials no autoritzat.
- Ús del correu electrònic corporatiu i personal.
- Programari permès o prohibit en els llocs de treball.
- Protocols d'ús dels equips informàtics per part dels empleats.

3.2. Altra normativa aplicable

Alguns incidents poden produir problemes legals que poden afectar a la imatge, el prestigi d'una empresa o el seu avantatge competitiu.

Per això, l'auditoria interna, com a procés que ha de vetllar per la protecció de la informació i els sistemes que la tracten, ha d'evitar el seu accés, ús, divulgació o destrucció no autoritzada, independentment del format en què aquesta es trobi.
És per això que també ha de tenir present les **lleis referents a la protecció de dades personals**, en especial aquelles catalogades com a sensibles perquè exigeixen una protecció especial (de salut, ideologia, condemnes penals o administratives,...).
D'aquesta manera, al mateix temps que es respecten els drets dels usuaris (proveïdors, clients,...) s'evita el cost, no tan sols econòmic, que pot suposar la comissió d'infraccions involuntàries.

Així, un atac a la privacitat el constitueix la divulgació d'informació confidencial o sensible, pel que una organització que no estigui preparada per complir amb aquests requeriments, pot haver de fer front a indemnitzacions i sancions econòmiques de quantia important pels danys i prejudicis soferts a l'afectat. A tot això, cal afegir d'altres efectes que perjudiquen a l'organització, com suposa la pèrdua del seu prestigi com a conseqüència d'aquest tipus d'incident.

A continuació s'exposen els principals delictes informàtics, que tant la legislació europea com l'espanyola, classifiquen en quatre grups diferents:

Delictes contra la propietat intel·lectual

- Afecten a la protecció dels drets d'autor, incloent bases de dades i programes informàtics.
- Exemple: Pirateig informàtic.

Delictes contra la intimitat

- Es produeixen quan es realitza un tractament de les dades de caràcter personal de forma il·legal, sense el consentiment de l'afectat.
- Exemple: Venda de dades a tercers sense l'autorització del seu propietari.

Delictes econòmics

- Inclouen els fraus, falsificacions i sabotatges que tenen lloc per mitjà de l'accés autoritzat als sistemes informàtics.
- Exemple: Suplantació d'identitat.

Delictes relatius al contingut

- Consisteixen en la difusió a través de la xarxa de continguts il·legals.
- Exemple: Difusió de pornografia infantil.

Figura 9. Classificació dels principals delictes informàtics

Cal puntualitzar que a l'hora de considerar els virus informàtics com a delictes informàtics, s'ha de tenir en compte que n'hi ha alguns que poden ser inofensius, però d'altres produeixen danys informàtics molt importants, arribant a destruir tant la informació com els actius que permeten tractar-la. Segons la legislació actual, la creació d'un virus informàtic per sí mateixa no es reconeix com a delicte, però tal com estableix l'article 264 del Codi Penal[8], en cas que produeixi danys, aquesta consideració canvia radicalment, convertint-se en delicte.

[8] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal [en línia]. [Consulta: 24 d'octubre de 2022]. <https://www.boe.es/eli/es/lo/1995/11/23/10/con>

Sigui com sigui, cal considerar sempre les mesures organitzacionals i tècniques que contribueixin a garantir els drets a la privacitat, a fi de reduir els perjudicis tant a terceres persones com a la mateixa organització. Així doncs, a l'hora de dur a terme una auditoria caldrà atenir-se a la següent legislació que li és aplicable:

- la **Carta de Drets Fonamentals de la Unió Europea**[9], proclamada a Niça el 7 de desembre de 2000, i el **Tractat de Funcionament de la Unió Europea**[10] (TFUE), estableixen que tota persona té dret a la protecció de les dades de caràcter personal que li concerneixen.

- **Reglament (UE) 2016/679 del Parlament Europeu i del Consell**[11], de 27 d'abril de 2017 (RGPD), relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades. D'aquesta normativa es poden destacar els següents aspectes:
  - S'informarà en tot moment al Delegat de Protecció de Dades quan es tractin dades personals, ja que aquest és el responsable de supervisar que s'està complint aquest reglament.
  - Si es detecta l'incompliment d'aquesta legislació, es disposaria d'un termini d'unes 72 h per a comunicar-lo a l'Agència Espanyola de Protecció de Dades i als afectats.
  - La designació d'un responsable de dades i un delegat de protecció de dades.
  - Analitzar la política de privacitat, que ha de ser transparent i oferir confiança als clients.
  - Complir els drets dels usuaris: aquests inclouen els drets d'accés, rectificació, cancel·lació i oposició (*ARCO*). A aquests, cal afegir els d'eliminació de les seves dades i el coneixement de la informació de què disposa l'organització, en quin moment els ha cedit o de quina manera s'han aconseguit.
  - L'emmagatzematge d'informació al núvol pot localitzar-se a servidors de països estrangers que no es regeixen per la legislació europea de protecció de dades personals. Per tant, si hi ha algun incident amb aquestes dades, seria l'organització la responsable i no els proveïdors del servei al núvol.

- **Reglament (UE) 2022/868 del Parlament Europeu i del Consell, de 30 de maig de 2022, relatiu a la governança europea de dades i pel qual es modifica el Reglament (UE) 2018/1724**[12] (Reglament de governança de dades): regula les condicions, per part

[9] Carta dels drets fonamentals de la Unió Europea [en línia]. [Consulta: 22 d'octubre de 2022]. https://barcelona.spain.representation.ec.europa.eu/publications/carta-dels-drets-fonamentals-de-la-unio-europea_ca

[10] Tratado de funcionamiento de la Unión Europea [en línia]. [Consulta: 22 d'octubre de 2022]. <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:C:2016:202:TOC>

[11] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) [en línia]. [Consulta: 20 d'octubre de 2022]. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>

[12] Reglament (UE) 2022/868 del Parlament Europeu i del Consell, de 30 de maig de 2022, relatiu a la governança europea de dades i pel qual es modifica el Reglament (UE) 2018/1724 (Reglament de governança de dades) [en línia].

del sector públic, de la reutilització de certes categories de dades protegides dins de la Unió Europea, però també el seu accés i transferència internacionals.
Per poder reutilitzar les dades, caldrà una sol·licitud al punt únic d'informació des d'on serà accessible la informació i es disposarà d'un termini màxim de 12 mesos per poder efectuar la reutilització sol·licitada.

A més, el reglament fixa que per garantir el compliment dels principis de confidencialitat, integritat, accesibilitat i privacitat de la informació, les dades es seudonimitzaran.

La prestació de serveis d'intermediació de dades exigirà als seus proveïdors una notificació, i en cas de no pertànyer a països de la UE, hauran de designar un representant legal en algun d'aquests països on s'ofereixin aquests serveis.

A més, es regula la cessió altruïsta de dades i les autoritats competents per inscriure al registre les organitzacions que gestionen aquestes dades.

Per altra banda, defineix les funcions d'assistència i assessorament del Comité Europeu d'Innovació en matèria de Dades pel que respecta a la cessió de dades, a la seva reutilització per part dels estats membres i el registre de les organitzaciones que tracten les dades amb una finalitat altruïsta.

- **Constitució Espanyola**[13], de 27 de desembre de 1978, limita l'ús de la informàtica per garantir drets com l'honor, la intimitat personal i familiar dels ciutadans.

- **Llei Orgànica de Protecció de Dades i Garantia de drets digitals (LOPDGDD)**[14]**:** amb aquesta llei s'adapta el RGPD de la Unió Europea a la legislació espanyola.
Segueix les línies generals de la llei d'àmbit comunitari en relació amb el tractament de les dades personals. Però també introdueix com a novetat la garantia dels drets digitals dels ciutadans segons l'establert per l'article 18.4 de la Constitució, pel que regula l'ús de les galetes o *cookies* i el consentiment actiu.

  Com succeïa amb la Llei Orgànica de Protecció de Dades (LOPD), que ja no és en vigor, es mantenen els drets d'accés, rectificació, supressió i oposició. Però se n'afegeixen de nous: els drets de limitació del tractament i a la portabilitat de les dades.

  Per al tractament de les dades personals es basa en el model de responsabilitat activa, consistent en l'avaluació prèvia de les dades que es volen tractar per part dels

[Consulta: 21 d'octubre de 2022]. <https://apdcat.gencat.cat/web/.content/01-autoritat/normativa/documentos/Data-governance-act.pdf>

[13] Constitució espanyola [en línia]. [Consulta: 22 d'octubre de 2022]. <https://www.senado.es/web/conocersenado/normas/constitucion/index.html?lang=ca_ES>

[14] Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals [en línia]. [Consulta: 20 d'octubre de 2022]. <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673>

responsables, i posteriorment, adoptar aquelles mesures que siguin necessàries per tractar-les.

És imprescindible el seu coneixement per les organitzacions perquè en cas d'incompliment les sancions a que s'exposen són quantioses: si una pàgina web utilitza alguna tecnologia (per exemple, les galetes) que processa les dades personals dels usuaris sense seguir les directrius establertes per aquesta llei, les sancions poden arribar fins als 20 milions d'euros, depenent de la gravetat de la infracció.

- **Llei Orgànica 34/2002 de Serveis de la Societat de la Informació i del Comerç Electrònic (LSSI)[15]:** per mitjà d'aquesta llei es regula el funcionament dels prestadors de serveis de la Societat de la Informació, les empreses que desenvolupen la seva activitat a través del comerç electrònic i aquelles que fan publicitat utilitzant mitjans electrònics.
  Segons aquesta llei, a les pàgines web és obligatòria la inclusió de la informació que identifica a l'empresa i els productes o serveis que ofereix.

- **Llei 17/2001 de Marques[16]:** segons la qual, el titular d'un nom comercial o d'una marca ha d'otorgar el seu consentiment prèviament a qui vulgui utilitzar-los en noms de dominis, a les xarxes telemàtiques i pàgines web.
  En cas contrari, el titular pot prohibir la seva utilització, ja que és qui disposa dels drets de propietat industrial.

- **Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (LPACAP)[17],** que va derogar l'antiga Llei 11/2007 d'Accés Electrònic als Serveis Públics.
  Aquesta llei regula els drets i les obligacions dels ciutadans a relacionar-se amb les Administracions Públiques mitjançant les noves tecnologies, així com també les relacions entre aquestes administracions a través d'aquests mitjans i el seu ús en l'activitat administrativa. Contempla tant els aspectes de la tramitació presencial com electrònica.

- **Llei 59/2003 de Signatura Electrònica[18]:** regula la prestació dels serveis de certificació, així com també l'eficàcia jurídica de la signatura electrònica, utilitzada per a la

[15] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico [en línia]. [Consulta: 23 d'octubre de 2022]. <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

[16] Ley 17/2001, de 7 de diciembre, de Marcas [en línia]. [Consulta: 23 d'octubre de 2022]. https://boe.es/buscar/act.php?id=BOE-A-2001-23093

[17] Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques [en línia]. [Consulta: 23 d'octubre de 2022]. <http://www.caib.es/sites/transparenciaperconselleria/ca/n/ley_392015_de_1_de_octubre_del_procedimiento_administrativo_coman_de_las_administraciones_pablicas>

[18] Llei 59/2003, de 19 de desembre, de signatura electrònica [en línia]. [Consulta: 22 d'octubre de 2022]. <https://portaljuridic.gencat.cat/ca/document-del-pjur/?documentId=668429>

identificació d'una persona en les transaccions electròniques i per reconèixer si ha existit alguna manipulació en el contingut del missatge.

- **Llei 32/2003 General de Telecomunicacions[19]:** és l'encarregada de regular el mercat de les telecomunicacions tal com indica el seu nom, fomentant el desenvolupament d'aquest sector i defensant els interessos dels ciutadans. Inclou la prestació dels serveis de comunicacions electròniques i l'explotació de les xarxes.

- **Reial Decret Legislatiu 1/1996 de Propietat Intel·lectual[20]:** que estableix que la creació d'una obra, ja sigui literària, artística o científica, fa que la propietat intel·lectual recaigui sobre el seu autor i que aquest tingui els drets exclusius de la seva explotació.
  Com que inclou les creacions d'obres originals en qualsevol mitjà, també afecta a les aplicacions i a les bases de dades que es fan servir a l'organització.

Cal destacar que aquestes lleis, tot i que vigents actualment, no s'adapten suficientment pel que respecta al món de la tecnologia, ja que aquesta avança a passos molt més agegantats i facilita als ciberdelinqüents eines molt més potents a les que donen un ús indegut i il·legal, de forma que en poc temps, apareixen nous delictes informàtics de tot tipus, i alhora, origina que el seu creixement resulti exponencial.

Aquests ciberdelictes poden dividir-se d'una banda, entre els que ataquen les infraestructures informàtiques i de comunicacions, i d'altra, els que s'aprofiten de la tecnologia per dur-los a terme:

[19] Ley 11/2022, de 28 de junio, General de Telecomunicaciones [en línia]. [Consulta: 22 d'octubre de 2022]. <https://www.boe.es/buscar/act.php?id=BOE-A-2022-10757>

[20] Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia [en línia]. [Consulta: 23 d'octubre de 2022]. <https://boe.es/buscar/act.php?id=BOE-A-1996-8930>

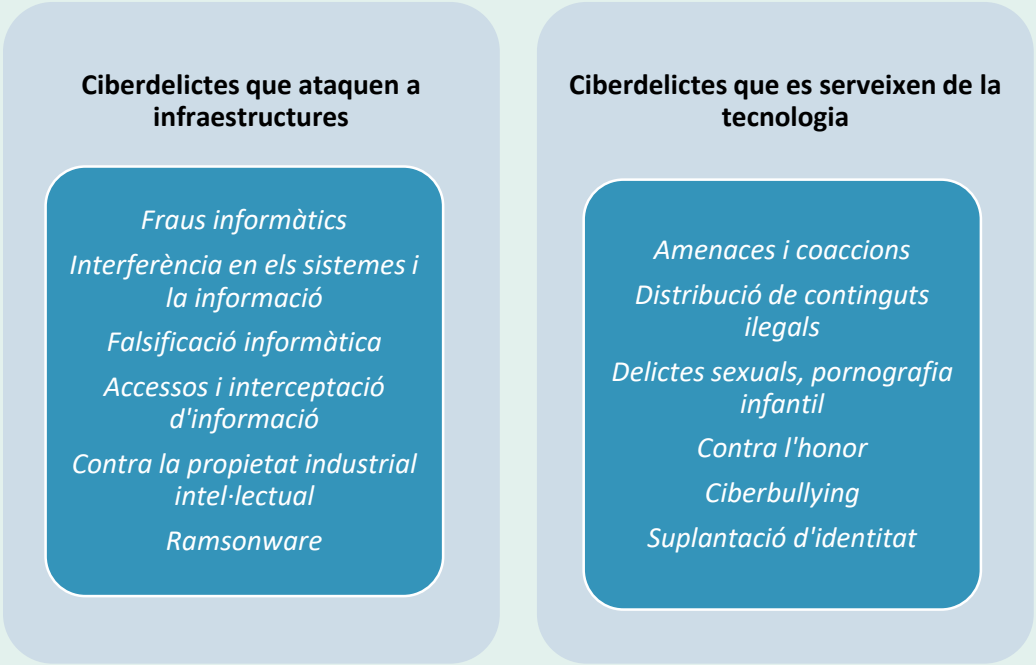


Figura 10. Classificació dels ciberdelictes

A més, a banda d'aquesta legislació que es pot aplicar de forma genèrica a qualsevol organització, també hi ha d'altra més específica i pròpia per alguns sectors.

Així, per exemple, dins de l'àmbit sanitari, és el cas de la llei 41/2002 de 14 de novembre[21] que regula l'autonomia del pacient i els seus drets i obligacions pel que fa a la seva informació i documentació clínica.

D'altres sectors, com el bancari, es recolzen inclús en legislació internacional, com la Llei de Resiliència Operativa Digital (*DORA*)[22] que estableix el marc regulatori i les recomanacions vers la seguretat de la informació que han de complir els països de la UE. Per mitjà d'aquesta llei, es preten que aquest sector implementi mesures tant per detectar possibles atacs com per respondre de forma adequada davant qualsevol incident, i en cas d'incompliment, es contemplen mesures penals.

[21] Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica ("BOE" 274, de 15 - 11 - 2002) [en línia]. [Consulta: 22 d'octubre de 2022]. http://www.boe.es/boe_catalan/dias/2002/12/02/pdfs/A03057-03062.pdf

[22] Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure [en línia]. [Consulta: 24 d'octubre de 2022]. <https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf>

4. Elaboració del pla d'auditoria

4.1. Presentació de l'auditor

L'auditor explicarà durant una reunió inicial amb la gerència la importància de l'auditoria i quines seran les tasques que desenvoluparà durant el seu procés.

En principi, durant aquesta reunió tractarà amb l'equip directiu, del que és fonamental obtenir el seu suport, els següents punts:

- **Presentar qui serà l'encarregat de l'auditoria**, que segons la seva magnitud pot ser desenvolupada per un únic auditor o per un grup d'auditors.
- **Exposar l'abast i els objectius** de l'auditoria, conscienciant als responsables de l'organització de l'existència de riscos i la necessitat de gestionar-los.
- **Informar del calendari** a seguir per complir amb la seva planificació, per si cal acordar algun canvi.
- **Les necessitats que caldrà cobrir per fer viable l'auditoria** (recursos, aportació de documents i procediments de seguretat,…)
- **Sol·licitar la implicació del personal** afectat per l'auditoria.

4.2. Identificació de l'abast i els objectius de l'auditoria

Cal estudiar de quina **situació actual** es parteix a l'empresa i l'entorn en què es troba.

Depenent de factors com que aquesta sigui més o menys gran, caldrà **definir si les activitats de l'auditoria es poden aplicar a tota l'organització** en general, o si interessa, degut al tamany de l'organització o altres raons, realitzar-les únicament **per determinades unitats o departaments** (ex. Àrea de Gestió documental, departaments de Finances, de Recursos Humans,...)

4.3. Estudi inicial de l'entorn a auditar

L'àrea de Tecnologies de la Informació de l'organització proporciona informació de primera mà ja que és més coneixedora de problemes de seguretat viscuts o disposa de major informació sobre necessitats o anomalies als sistemes informàtics.

Per això, una de les primeres visites es dirigiria a l'àrea TIC de l'organització per reunir-se amb el personal destinat únicament a tasques informàtiques (per exemple, coordinadors dels sistemes informàtics, de telecomunicacions,...).

D'aquesta manera es disposaria d'informació molt diversa:

- sobre possibles mancances detectades,
- possibles accions de millora,
- necessitats dels usuaris vers aplicacions informàtiques,
- tipologia de les incidències,
- activitats formatives que el personal deuria rebre per poder ampliar o actualitzar els seus coneixements,...

4.4. Determinació dels recursos implicats en l'auditoria interna

Els actius implicats a l'auditoria interna són tots aquells recursos d'informació, que en conjunt, permeten el bon funcionament de l'organització i contribueixen a l'assoliment dels seus objectius.
Tal com s'exposa a continuació, són molt diversos, ja que van des d'aquells recursos materials, com poden ser els equips tecnològics i les infrastructures que possibiliten el seu funcionament, fins als recursos humans, és a dir, els empleats que utilitzen els primers per gestionar la informació i desenvolupar els processos de negoci.

4.4.1. Recursos humans

Tot i que sigui l'auditor qui en realitat executa de forma directa l'auditoria, tots els recursos humans tenen un paper cabdal dins d'aquest procés.

4.4.1.1. Personal directiu

És el personal responsable de l'organització que pot requerir l'auditoria interna. Es constitueix com el recurs que **ha de liderar aquest procés** perquè coneix de primera mà quins són els riscos de la seva activitat a nivell legal, financer, les obligacions amb els seus clients, la relació amb els seus proveïdors i socis,...

És molt important que, de forma conjunta amb el personal auditor i els responsables amb competències sobre la seguretat del sistema d'informació, estableixin abans de començar el procés auditor, quins són els seus objectius. A més d'aquests, també hauran d'acordar i documentar quin és el seu abast, ja que les mesures de seguretat a auditar poden incloure elements de naturalesa molt diversa (organitzatius, físics, lògics,...)

Cal tenir en compte que el paper de la Direcció en les polítiques de seguretat és necessari perquè és qui proporciona les directrius que permeten posteriorment als equips tècnics desenvolupar les tasques per gestionar la seguretat informàtica.
Per exemple, proporcionen informació sobre els requeriments que han de complir els llocs de treball per tal de desenvolupar les seves tasques. D'aquesta manera, es dóna l'orientació per

dissenyar els rols per a que els usuaris disposin dels privilegis mínims per garantir la realització de les seves tasques adequadament i la gestió de les contrasenyes per a que siguin el més segures possible.

4.4.1.2. Personal encarregat de l'auditoria

És convenient que a fi de reduir el cost econòmic per a l'empresa de seleccionar com **auditor/s a una persona de la pròpia empresa**, que deuria de ser independent dels sistemes, departaments o serveis que han de ser auditats a fi d'assegurar la seva objectivitat. Per exemple, les tasques podrien ser desenvolupades anualment per un auditor pertanyent a un departament d'Auditoria o de Control intern.

Però a més, tot el que implica el desenvolupament d'un procés auditor fa imprescindible que aquesta disposi dels coneixements i les capacitats necessàries per poder revisar temes tècnics i tecnològics per poder desenvolupar aquesta funció amb garanties: seguretat de les comunicacions, plans de continuïtat, ús d'eines per realitzar comprovacions,...

Cal considerar que entre les seves funcions es troben les següents:

- **La participació en les revisions** al llarg de totes les etapes de l'auditoria (disseny, execució, recomanacions,…)
- **Revisar que els sistemes informàtics compleixen amb els requeriments legals** de protecció de la confidencialitat, de les directrius establertes per la gerència, de fiabilitat i seguretat,…
- **Assessorar i proporcionar mesures correctives** per reduir o evitar possibles deficiències.
- **Vetllar pel compliment** de les polítiques, estàndards, normes i els procediments de seguretat informàtica establerts per l'organització.

Segons l'abast de l'auditoria podria caldre la **incorporació d'altres perfils especialitzats**, com poden ser els dels experts amb coneixements jurídics i legals, sobre els procediments establerts per les direccions tant de l'empresa com l'encarregada dels sistemes d'informació, o referents a la gestió documental i els arxius electrònics, entre d'altres.

A tot això, cal afegir que és molt convenient que el personal encarregat de l'auditoria, abans de començar-la, tant si és intern com si incorpora algun professional extern en alguna matèria que no es pot cobrir amb personal de la pròpia organització, signi un **acord de confidencialitat** que inclogui clàusules aplicables de la normativa sobre tractament de dades de caràcter personal.

Segons la grandària de l'organització, per al desenvolupament de l'auditoria interna, l'auditor en pot planificar diverses al llarg de l'any distribuïdes per departaments, de forma que la resta continuïn amb la seva activitat diària amb normalitat.

4.4.1.3. Resta d'empleats de l'empresa

Tot i que els directius i el personal tècnic i informàtic proporcionaran informació que altres àrees i departaments no podran facilitar, també resultarà molt valuosa la que es pot obtenir a través de la retroalimentació amb la resta d'empleats i personal de base de l'organització.
Sobretot resulta interessant perquè, en general, la producció d'un servei o un producte implica una sèrie de processos de negoci diferents, pel que no tot el personal desenvolupa les mateixes tasques i per tant, poden utilitzar actius diversos. Per tant, cal conèixer les **responsabilitats i les funcions que desenvolupen** a fi d'orientar d'una forma més adequada les consultes i les proves que més endavant es duran a terme.

A més a més, sota el seu punt de vista, poden exposar aspectes que es podrien millorar quant a procediments de tractament d'informació per tal d'aconseguir major eficiència o **descobrir mancances en recursos materials o dels aplicatius** que incideixen directament en la seguretat.
Així mateix, l'auditor podria recollir dubtes que permetrien detectar **necessitats formatives** per, més endavant, orientar al Departament de Recursos Humans en el desenvolupament d'accions enfocades vers aquestes.
A més, cal tenir en compte que molts atacs aprofiten les vulnerabilitats socials, i no únicament les tècniques, pel que bona part de la seguretat depèn del comportament del personal dins d'aquest àmbit. Per això, l'auditor hauria de **comprovar personalment com es desenvolupen les tasques** i extreure conclusions entorn a si tothom segueix un criteri unificat o homogeni per treballar amb la informació, basat en el compliment dels estàndards o les metodologies establertes.

De la mateixa manera, durant l'auditoria es pot comprovar *in situ* el nivell **de sensibilització pel que fa a la seguretat informàtica** i si aquest àmbit representa o no una prioritat. En referència a això, es destaca la importància de conèixer quin procediment segueixen els usuaris per gestionar els incidents en seguretat informàtica.

4.4.2. Recursos materials/tecnològics de l'entorn auditable

4.4.2.1. Instruments de recol·lecció de la informació per l'auditoria interna

Aquests instruments permetran obtenir bona part de les dades necessàries per poder analitzar els procediments i els equipaments que componen els sistemes d'informació.
Com a recursos que poden proporcionar una informació molt valuosa es troba la **documentació** que es pot obtenir de cadascun dels departaments de l'empresa, que en conjunt proporcionarà a l'auditor una visió propera de l'estat de seguretat informàtica abans de començar l'auditoria.
Però també n'hi ha d'altres, com les **entrevistes**, el **programari per realitzar proves** o els **qüestionaris**, que ens permetran obtenir aquella informació que no es pugui obtenir a partir de documents.

Com que caldria recollir documentació que pot ser força nombrosa i diversa, és aconsellable que l'organització, per tal de no comprometre el calendari de l'auditor, la faciliti amb l'antelació

suficient. De fet, el volum de documents que s'han de recopilar és molt abundant, com s'exposa a continuació, tot i que també cal comptar que és possible que alguns documents siguin inexistents o incomplets:

- **Polítiques i procediments de seguretat** que deurien estar convenientment actualitzades per garantir la seguretat, amb l'enumeració de les mesures implantades pels requeriments legals o pel fet d'haver identificat riscos. Deurien incloure informació sobre quins elements s'aplica, responsabilitats, objectius, requeriments mínims de configuració i sancions en cas d'incompliment. Aquestes polítiques poden tractar l'ús del correu electrònic, les actualitzacions de noves aplicacions o equips, l'ús de dispositius externs o de les unitats de xarxa per a l'emmagatzematge d'informació,…

- **Organigrames** de les àrees a auditar, amb el detall de les funcions i responsabilitats dels seus components.

- En cas de disposar-ne, els **informes d'auditories de seguretat anteriors**, i els corresponents **informes de seguiment** de les mesures correctores aplicades.

- **Polítiques de còpies de seguretat de la informació i de les bases de dades** amb el detall de la periodicitat i el tipus de còpia amb la que es realitzen.

- **Plans de contingència** davant de desastres, que permetin dur a terme les accions de recuperació necessàries per reduir les pèrdues i reanudar l'activitat a la situació anterior com es trobava a l'incident. Haurà de contenir el detall de qui realitza les accions, amb els recursos i el moment en què s'han de realitzar.

- **Plans de gestió de la continuïtat del negoci** que serveixin com a guia per realitzar un seguiment adequat de les accions a executar després d'un incident de seguretat.

- **Estratègies de desenvolupament de proves prèvies** a la implementació d'una aplicació en la fase de producció.

- Descripció tant de les **accions formatives** dirigides als treballadors afectats per l'auditoria com dels **programes de conscienciació** adreçats a diferents usuaris (clients, proveïdors, empleats) en relació a la seguretat.

- **Polítiques de seguretat** que afecten a **dispositius d'ús personal** (BYOD)[23] donat el seu creixent ús.

- **Registre o llistat d'incidències** dels sistemes informàtics (tant a nivell lògic com físic).

[23] Decálogo ciberseguridad empresas: una guía de aproximación para el empresario [en línia]. [Consulta: 25 d'octubre de 2022]. https://www.incibe.es/protege-tu-empresa/blog/decalogo-ciberseguridad-empresas-guia-aproximacion-el-empresario

- **Polítiques de control** d'accés lògic, de retorn d'actius d'informació si l'empleat marxa de l'organització,...
- **Registres del logs i informes** de detecció i enregistrament de successos.
- **Llistats de personal** que ha ocasionat baixa o ha marxat recentment de l'empresa.
- **Procediment disciplinari i responsabilitats** dels empleats després d'extingir el contracte.
- **Polítiques de signatura electrònica, certificats digitals i xifrat de dades**.
- **Protocol a seguir pels usuaris que realitzen teletreball** o treball amb dispositius mòbils fora de l'organització.
- **Contractes** amb informació sobre quina mena d'activitats es desenvolupen, encaminades a proporcionar el **manteniment preventiu i correctiu** del maquinari com també d'aquelles mesures correctores o de millora del programari i de les aplicacions corporatives. Han d'incloure els **acords de nivell de servei**, que indiquin de forma detallada aspectes tan importants com el de la freqüència amb la que es realitzen aquestes activitats o els temps de resposta davant una incidència.
- **Llistat de tots els proveïdors i col·laboradors** que ofereixen serveis a l'organització i que poden entrar dins de l'abast de l'auditoria.
- **Contractes de confidencialitat** amb els proveïdors que proporcionen els serveis que garanteixin la confidencialitat, disponibilitat i integritat de la informació per evitar el seu ús fraudulent.
- **Llistat amb la classificació de la informació** existent o circulant dins de l'organització, amb indicació del seu nivell de transcendència i protecció, per a quines funcionalitats resulta útil i quins són els departaments que, per poder desenvolupar la seva activitat, necessiten accedir per efectuar el seu tractament.

4.4.2.2. Inventari dels recursos informàtics

4.4.2.2.1. Maquinari

Cal revisar l'inventari on s'identifiquen i classifiquen tots els actius que formen part del maquinari.

En aquest inventari, ha de constar el detall de la marca i model del dispositiu, el número de sèrie, l'adreça MAC i l'ús que se'n fa. També és important que inclogui la seva ubicació (departament, planta de l'edifici,…) i, si és possible, obtenir informació sobre quins són els responsables assignats a cadascun d'aquests actius.

Així mateix, cal **distingir aquell que presenta major criticitat**, bona part del qual es correspon amb la infrastructura de la xarxa (servidors, elements de comunicació, armaris de telecomunicacions, suports d'informació,...) o si és maquinari destinat a desenvolupar unes tasques específiques dins dels processos de negoci de l'organització (equips d'escriptori, multifuncions, impressores,…).

A més, cal comprovar la possible existència **d'equipament de reserva o *backup*** *i* tenir en compte els equips portàtils que surten fóra de l'organització degut a la creixent expansió del teletreball.

Tampoc cal oblidar dispositius com els punts d'accés que proporcionen **connexió a la xarxa Wifi**. Aquests han de ser configurats amb un SSID específic en el cas que calgui proporcionar accés a persones externes a l'organització. És convenient disposar de documentació sobre el límit d'amplada de banda que permeten, el sistema de xifrat utilitzat per accedir-ne, si existeix filtratge del tipus de pàgines que es poden visitar a través d'aquesta xarxa, nombre d'equips que es poden connectar,…

En resum, deuria obtenir-se tota la informació mínima referent al cicle de vida d'aquest maquinari:

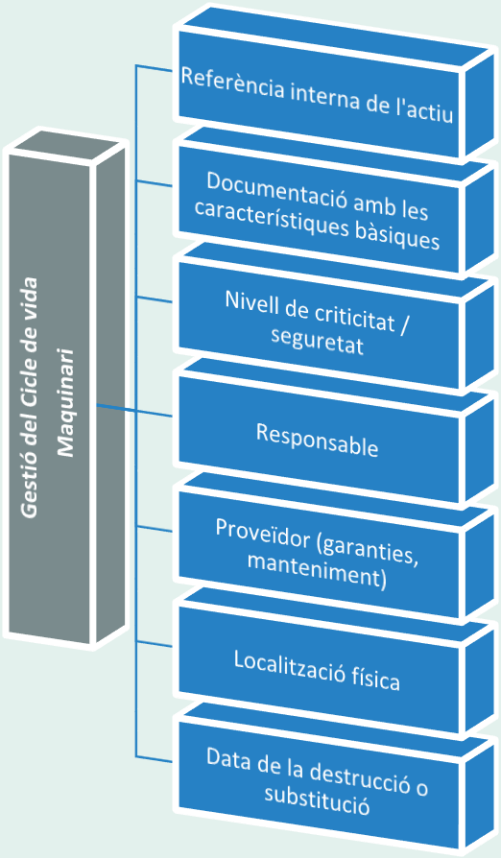


Figura 11. Gestió del cicle de vida del maquinari

4.4.2.2.2. Programari i informació

De la mateixa manera que succeeix amb el maquinari, cal disposar d'un inventari actualitzat de totes les aplicacions existents i permeses, a fi, entre d'altres raons, d'evitar l'execució de codi maliciós.
Juntament amb aquest llistat, ha d'aparèixer el detall de les seves versions actuals, les dates de properes actualitzacions, les adquisicions de nou programari, les llicències i els usuaris que en fan ús o estan autoritzats atenent a aspectes com són el departament i el lloc de treball que ocupen.

El programari pot incloure des de **les aplicacions específiques** de cadascun dels departaments d'una organització, passant pels **paquets ofimàtics, navegadors, gestors de bases de dades i els sistemes operatius** dels equips dels empleats i dels servidors, fins aquell encarregat de proporcionar **seguretat a la xarxa** (antivirus, tallafocs,...)

Tampoc cal oblidar la **informació utilitzada en l'activitat diària** de l'organització i que es pot trobar en diferents suports i formats, pel que l'auditor haurà de conèixer diferents aspectes referents a la seva gestió:

- *Documentació sobre els plans de còpia de seguretat i recuperació*, que inclogui les versions, responsabilitats, freqüència d'execució,...
- *Detall dels formats, dispositius* (taxes de transferència, durabilitat, capacitat) *i ubicacions* destinats al seu emmagatzematge que compleixin amb les condicions ambientals per a la seva conservació òptima.
- *Mesures de protecció* que s'apliquin quan la informació s'emmagatzemi o surti físicament de les instal·lacions per garantir la seva confidencialitat i integritat.
- *Identificació física i lògica* dels suports extraïbles.
- *Registre dels moviments* dels suports d'informació: persona que el fa servir, data d'entrada i sortida,…
- *Control de l'accés a la informació*: permisos segons les necessitats funcionals, perfils dels usuaris,…
- *Emmagatzematge segur* de la informació que hagi de romandre permanentment per qüestions legals.
- *Control de la informació* ubicada al núvol.
- *Protocol de destrucció* de la informació quan finalitzi la seva vida útil.

Per altra banda, resultarà molt útil conèixer per a quins processos de negoci es fan servir les aplicacions, el seu grau d'interoperabilitat amb la resta i la seva dependència respecte d'altres sistemes, per avaluar en cas d'indisponibilitat d'aquests, si el flux d'informació es veurà afectat o, sí pel contrari, existeix alguna alternativa per evitar la interrupció del servei.

4.4.2.2.3. Equipament de la infrastructura de xarxa

Per a que una xarxa sigui segura cal que tot els components que en formen part estiguin configurats adequadament i es monitoritzin per detectar errors o anomalies i garantir en la mesura del possible, que tots funcionin ininterrompudament per assegurar la seva disponibilitat i un bon rendiment.

Tot i ser un equipament menys visible, en comparació amb el que es pot trobar a les oficines, no és gens menys important, ja que és l'encarregat de permetre la interconnexió dels sistemes d'informació entre sí a través de la xarxa interna i amb d'altres xarxes externes, amb el que augmenta la seva complexitat.
Cal verificar **la seva administració i la introducció de les mesures necessàries** per a que la infrastructura de xarxa mantingui la seguretat dels sistemes i aplicacions per evitar intrusions.
El seu bon funcionament exigeix una correcta configuració dels seus dispositius que només pot ser accessible per personal autoritzat i ha de complir amb els estàndards de comunicació.
Així mateix, la seva **monitorització** permet avaluar que el rendiment és òptim o, que pel contrari, indiqui la necessitat de realitzar canvis per dimensionar la xarxa; descobrir possibles problemes en algun d'aquests dispositius que poden desembocar en la degradació del servei, i fins i tot, detectar la presència d'intrusions o atacs a la xarxa.

A més, cal comprovar l'existència de registres conforme els quals es demostri que aquests **equips són revisats periòdicament**, per detectar qualsevol problemàtica relacionada amb les configuracions o possibles incidències en el seu funcionament i evitar un empitjorament de l'avaria que comprometi la disponibilitat de la xarxa.
Per facilitar una reconfiguració d'aquests dispositius en el menor temps possible, cal comprovar que es disposa de **còpies de seguretat dels arxius de configuració** i la corresponent **documentació convenientment actualitzada**.

Entre els dispositius de xarxa sobre els que l'auditor haurà d'obtenir informació es troben principalment:

- **Encaminador (router):**

  Cal comprovar que aquests dispositius de capa 3 tenen configurades **rutes alternatives** amb tots els segments de xarxa per evitar en la mesura del possible que el servei no quedi interromput.

  Per garantir una major protecció davant d'atacs, cal comprovar que es duen a terme una sèrie de mesures:

  - Ús de protocols segurs com SSH o SCP, enlloc d'altres que tot i ser equivalents resulten insegurs.
  - Autenticació per mitjà de MD5 per evitar connexions no autoritzades.
  - Firmware i IOS actualitzats.

○ Habilitar els logs i protocols per analitzar qualsevol anomalia o fer-ne seguiment. ○ Deshabilitar els serveis i els ports innecessaris. ○ Registres de les modificacions de la configuració. ○ Ús de protocols per autenticar les sessions d'administració. ○ Eliminar les configuracions per defecte i contrasenyes robustes.

Taula 5. Algunes mesures de protecció davant d'atacs

- **Commutador (switch):**

Per garantir la disponibilitat d'aquests dispositius de capa 2, hauran de configurar-se com a **sistemes de mirall o en clúster**.

Caldrà revisar que segueixen una sèrie de mesures per millorar la seva seguretat:

○ Cal que les interconnexions entre commutadors siguin redundants. ○ Com qualsevol equip connectat a la xarxa, haurà d'estar actualitzat amb la darrera versió i habilitar només els ports necessaris per administrar-lo. ○ Definir els nivells de la xarxa troncal, distribució i accés. ○ Comprovar que es canvien periòdicament les contrasenyes i la velocitat d'accés per defecte. ○ Registrar els logs. ○ Utilitzar commutadors que siguin gestionables. ○ Desactivar els protocols innecessaris i xifrar el tràfic en la mesura del possible. ○ No utilitzar les VLAN per defecte i assignar una VLAN d'administració.

Taula 6. Mesures per millorar la seguretat dels commutadors

- **Tallafocs (firewalls):**

Com a equips que protegeixen el perímetre de la xarxa de l'organització a través de diverses funcionalitats, és molt aconsellable que s'estiguin utilitzant sistemes d'alta disponibilitat.

Entre els aspectes que caldrà verificar que es compleixen en la seva implementació es troben:

○ Actualització del firmware o el programari amb la darrera versió. ○ Ha de proporcionar permisos només al tràfic autoritzat, per exemple, la navegació per pàgines web segures o necessàries per desenvolupar l'activitat empresarial. ○ Monitorar i efectuar registres tant de l'activitat permesa com de la que no hagi estat autoritzada per identificar possibles intents d'atac. ○ Comprovar que el tràfic està separat per VLAN. ○ Els servidors principals s'han de trobar a la zona desmilitaritzada (DMZ).

○ Per garantir el suport dels fabricants cal mantenir convenientment actualitzades les llicències. ○ Utilitzar les opcions d'autenticació i xifrat i els clients VPN més segurs. ○ Cal habilitar al màxim nivell de seguretat les proteccions contra atacs a la xarxa i evitar ports oberts innecessaris.

Taula 7. Mesures per millorar la seguretat dels tallafocs

- **Servidors:**

S'ha de comprovar que les aplicacions i el seu sistema operatiu **s'actualitzen amb les darreres versions estables**.

A més, cal analitzar quines mesures es prenen per a la **monitorització** d'aquests equips a fi de conèixer en tot moment el seu estat. També s'inspeccionaran els **registres dels logs** per obtenir qualsevol informació que indiqui la possibilitat d'una incidència o una activitat estranya que podria ser compatible amb una intrusió.

Es verificaran d**'altres mesures conduents a la seva protecció**, com la seva inclusió dins de la DMZ de la xarxa; l'utilització de IDS per detectar alguna activitat no autoritzada; la monitorització dels serveis i els ports en ús; el xifrat de l'informació de les seves bases de dades o d'altres per assegurar la disponibilitat del servei, com pot ser l'existència de servidors de reserva que es posin en funcionament en cas d'incidència als principals.

- **Xarxes inalàmbriques:**

Moltes xarxes empresarials inclouen connexions en les que els equips accedeixen sense utilitzar com a mitjà transmissor el cable, com és el cas, per exemple, de les Wifi.

Això les fa **molt vulnerables a atacs, pel que cal configurar-les** de forma que s'eviti un accés indesitjat:

○ El nom de la xarxa deuria estar ocult per dificultar la seva identificació. ○ La contrasenya d'accés ha de ser robusta i actualitzar-se periòdicament. ○ Monitorar el tràfic d'aquestes xarxes. ○ Modificar les credencials d'administració que arriben per defecte de fàbrica. ○ La informació s'ha de xifrar amb protocols segurs. ○ Efectuar un control d'accés per mitjà de la MAC de l'equip que estigui autoritzat i controlar els usuaris connectats.

Taula 8. Mesures per evitar atacs a les xarxes inalàmbriques

A banda dels anteriors components de la xarxa, també cal parar atenció a aquell equipament que garanteix el subministrament energètic, com és el cas dels sistemes d'alimentació

ininterrompuda (SAI), que han de localitzar-se en llocs accessibles en qualsevol moment que sigui necessari i dels que s'haurien de fer constar els seus manteniments periòdics a un lloc visible.

4.4.2.2.4. Disseny lògic del sistema d'informació

El disseny lògic defineix l'arquitectura de la xarxa. Per a que aquest sigui fiable i funcioni perfectament, haurà de complir, almenys, amb els següents **principis bàsics**:

* Tolerància a errors: caldrà auditar l'existència de mecanismes o dispositius encarregats de minimitzar o evitar l'impacte que pot originar una deficiència del maquinari o el programari en el sistema, i si escau, permetre la seva recuperació al més aviat possible.

* Qualitat del servei (QoS): per desenvolupar les tasques de forma òptima cal administrar recursos de xarxa, com per exemple, l'amplada de banda, establint unes prioritats, ja que n'hi ha que requereixen un major nombre de serveis que han de trobar-se disponibles per evitar la degradació o la latència en la transmissió de la informació.
Per tant, durant l'auditoria es deuria considerar com administren el tràfic de dades els encaminadors i commutadors de la xarxa.

* Escalabilitat: en cas de necessitats de l'organització, la xarxa ha de donar resposta amb un rendiment raonable amb la introducció tant de nous sistemes i equips, com de clients o usuaris que s'hagin de connectar. Aquesta ampliació no ha de suposar un perjudici per a la xarxa.
Davant la constant evolució, tant de les activitats empresarials com dels mitjans tecnològics, l'auditoria ha de contemplar quina és la viabilitat d'un creixement a mig o llarg termini que no posi en risc la seguretat de la resta d'elements en xarxa.

* Seguretat: és altra característica dins de l'arquitectura de xarxa de la que es podria dir que és principal, degut a la dependència de les anteriors en cas que aquesta falli.
Així, no es podria parlar d'una bona tolerància a errors o qualitat del servei, ni tampoc pensar en escalar la xarxa, si es trenca la seva seguretat.
Això fa necessari auditar que els sistemes de seguretat existents, tant físics com lògics, es trobin actualitzats.
A més, cal observar si en l'esquema de l'arquitectura de xarxa queda detallada la incorporació de mecanismes per monitoritzar, controlar i evitar possibles intrussions:

    - tallafocs per controlar les entrades i sortides dins de la xarxa,
    - sistemes criptogràfics,
    - segmentació per reduir errors i atacs maliciosos,
    - DMZ,...

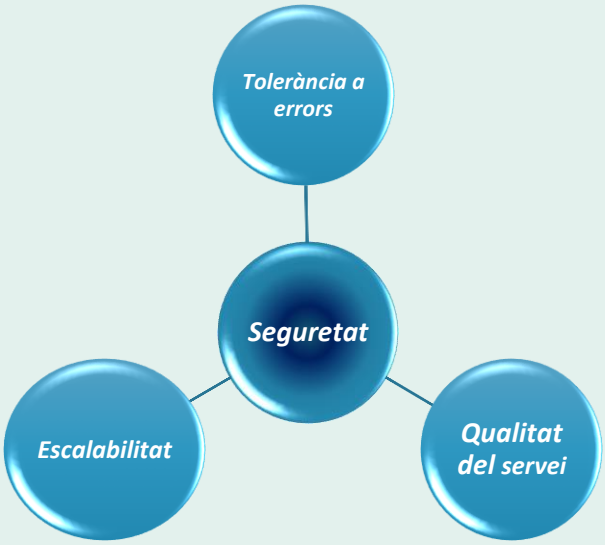


Figura 12. Principis bàsics del disseny lògic del sistema d'informació

A més, tal com es recomana des de l'INCIBE, cal tenir en compte els següents aspectes per valorar si el disseny de l'arquitectura de xarxa va en consonància amb els principis bàsics abans esmentats. D'aquesta manera, l'arquitectura de xarxa s'adaptarà a possibles necessitats actuals i futures de l'organització, i alhora, contribuïrà a aportar una major seguretat als sistemes informàtics que la integren:

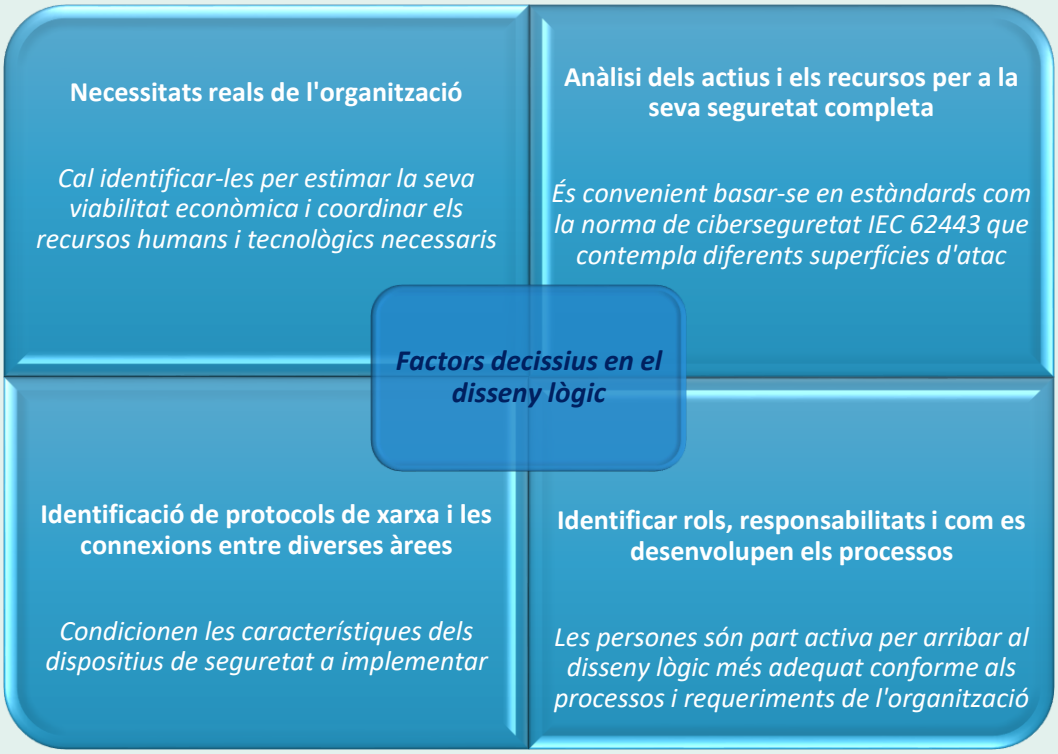


Figura 13. Factors decissius en el disseny lògic del sistema d'informació

Cadascun dels components d'una xarxa empresarial qualsevol compleix amb una funció i es poden distribuir seguint topologies diverses que, segons els propòsits de cada organització, poden contribuir a millorar el seu rendiment, o pel contrari, reduir la seva eficiència i afectar també a la seva seguretat. Per això, és fonamental avaluar el seu disseny per descobrir si realment s'està obtenint el benefici que s'esperava dels mitjans tecnològics disponibles o per contra, caldrà un redisseny que compatibilitzi els interessos empresarials amb els de seguretat, rendiment, disponibilitat,...

A més, cal comprovar que aquesta arquitectura sigui gestionable i escalable, de forma que permeti en el futur qualsevol canvi o l'ampliació amb nous equips.

Per tant, caldria revisar molts aspectes per reconèixer si els equips interconnectats es coordinen de forma que resultin útils a l'organització, però al mateix temps, que comptin amb garanties de seguretat.

Així, del seu disseny es podrien analitzar entre d'altres:

- tots els seus dispositius i els recursos que s'han de protegir, diferenciant aquells que presenten major criticitat per l'organització per la seva importància a l'hora de suportar l'activitat i per presentar un major nivell de risc,
- el número d'usuaris que han d'accedir per analitzar si la xarxa està suficientment dimensionada,
- els mètodes d'accés a la xarxa,
- les necessitats d'amplada de banda per atendre les operacions o els processos sense interrupcions,
- els mecanismes i els sistemes de seguretat i de control implementats,...

Taula 9. Aspectes a revisar de l'arquitectura de xarxa

El disseny ha de quedar documentat de forma detallada i precisa, i haurà d'incloure tots els elements que integren la xarxa i els actius de l'organització.

És convenient que el disseny proporcioni, de forma gràfica, informació sobre com circula el flux d'informació dins de la xarxa per reconèixer quins components hi estan involucrats.

Respecte al punt anterior, l'auditor ha d'estudiar els mecanismes de redundància de què es disposa per assegurar que aquest flux no quedi interromput davant qualsevol contingència, o en cas contrari, conèixer quin seria el grau d'afectació per a l'activitat.

A més, per a l'auditoria interna caldrà analitzar els procediments per cadascun dels components de la xarxa, si existeix un registre que inclogui les seves configuracions abans i després de la seva instal·lació, així com també quins són els seus responsables.

Per altra banda, cal tenir en compte que els dispositius que componen la xarxa poden trobar-se interconnectats a través de la combinació de més d'una de les possibles tecnologies existents,

ja que hi ha de diverses: des de connectar-se per mitjà de l'habitual xarxa cablejada, fins d'altres molt eficients com la fibra òptica, o les que ni tan sols es serveixen del cable per establir comunicació, com pot ser la tecnologia microones o la wifi.

En aquest sentit, el disseny ha d'indicar si la xarxa empresarial és únicament cablejada o inalàmbrica, o si és mixta, és a dir, que combini tant àrees cablejades com inalàmbriques, perquè el medi físic que les connecta comporta diferents exigències que repercuteixen en les mesures de seguretat que hauria de tenir implementades.

Cal observar que el disseny lògic d'algunes xarxes d'organitzacions de gran tamany pot ser força complex. Per això, deuria d'estar documentat amb el màxim detall possible, mostrant entre d'altres: la descripció de les VLAN que agrupen els equips de cadascun dels departaments, la separació de les xarxes Wifi de les cablejades, els equips inclosos dins de la zona desmilitaritzada (DMZ), els dominis de col·lisió,...

En la documentació d'aquest disseny haurien de quedar reflexats els segments físics de la xarxa que són molt recomanables per a la millora de la seva seguretat per diferents raons:

- **Milloren l'amplada de banda** al dividir els dominis de col·lisió en d'altres més petits o prioritzant-lo per als dispositius i aplicacions més exigents.
- **Per aïllar els equips amb major criticitat** en previsió d'un possible atac informàtic i reduir la infecció d'un atacant si alguna àrea de l'organització es veu afectada.
- **Reduir l'afectació sobre funcions** de determinades àrees que sense la segmentació es podrien veure afectades si el tràfic amb dispositius que possibiliten l'execució d'altres es troba interromput.

També és important que l'auditor revisi que tant el maquinari com el programari que apareixen reflexats en el disseny lògic permetin diferenciar la separació de funcions que desenvolupen els usuaris dels diferents departaments o que en fan ús d'unes aplicacions específiques, de forma que ajudi a agilitzar qualsevol canvi que s'hagi d'implementar.

Aquest disseny deuria informar dels protocols utilitzats per possibilitar el funcionament de xarxa, ja que caldrà valorar el seu nivell de seguretat, així com també dels privilegis de l'administrador per poder realitzar modificacions i manteniment de la xarxa, així com les operacions autoritzades per tal d'administrar la seguretat.

Respecte a la compartició dels recursos de la xarxa, a l'auditoria s'ha de valorar que és l'adequada en funció de les activitats que es desenvolupen i que es realitza de forma segura i eficient. En aquest sentit, a banda dels recursos compartits com poden ser els equips multifunció o les unitats de xarxa per emmagatzemar i compartir documentació, cal parar atenció a altres elements que són compartits. És, per exemple, el cas de les bases de dades, que poden presentar un ampli abast als diferents departaments de l'organització, ja que poden interconnectar-se amb diversos sistemes o aplicatius al mateix temps que extreuen informació a través d'aquestes.

4.4.2.2.5. Dependències entre les aplicacions dels diferents departaments

Una vegada identificats els recursos de programari, cal **identificar les dependències existents** entre tots ells, de forma que es pugui valorar i preveure que en cas d'incident amb algun d'aquests actius, quins altres es podrien veure afectats. A més, per mitjà de la seva identificació es podrà valorar el nivell de rellevància de cadascun dels actius, ja que no tots generaran el mateix impacte per a l'organització davant d'un atac.

Cal afegir que de l'estudi de la interrelació existent entre les aplicacions, dependrà en gran mesura **l'estratègia de seguretat a seguir** per desenvolupar accions d'adquisició, manteniment o desenvolupament, ja que depenent de les necessitats del negoci els requeriments de seguretat seran uns o altres i es podran ajustar de forma més eficient.

D'entre els aspectes que l'auditor haurà de conèixer amb major profunditat per analitzar les dependències entre les diferents aplicacions empresarials, es troba tota aquella informació relativa als procediments i processos que es desenvolupen amb aquestes, així com saber quins són els seus responsables o els usuaris habituals.

Cal dir que **la detecció d'aquestes dependències pot resultar una tasca encara més complexa** per altres situacions com poden ser:

- les d'aquelles organitzacions que han realitzat fusions amb altres companyies que segueixen criteris de seguretat informàtica diferents i, que a més, encara no han integrat tots els seus sistemes o es troben en ple procés de fer-ho.

- les relacions amb els proveïdors externs que ofereixen els béns i serveis, ja que en moltes ocasions aquests han d'accedir a informació confidencial i de clients o als propis sistemes d'informació de l'organització. En aquest cas, l'auditoria interna deuria d'analitzar, a més, diferents aspectes com: quina informació estan utilitzant tercers, de quina manera es transmet, com s'emmagatzema i com la processen,...
  Tot això, amb l'objectiu d'avaluar si per a l'organització són proveïdors d'alt risc o segurs.

5. Pla de treball de l'auditoria

5.1. Disseny de les entrevistes

Com a part essencial d'un procés auditor, cal tenir en compte **el factor humà**. Per tant, es realitzaran entrevistes i reunions amb usuaris dels sistemes d'informació que ocupin diferents nivells dins de la jerarquia empresarial ja que s'han de contemplar els diversos punts de vista i les formes de desenvolupar les seves funcions. Tot això, amb l'objectiu de detectar fonts de risc

per a la seguretat informàtica, com poden ser el desconeixement o una manca d'organització o de coordinació a l'hora de desenvolupar els seus processos.

Depenent de l'usuari a entrevistar s'hauran de dissenyar amb **preguntes diferents o més específiques del càrrec que ocupen** (cap d'informàtica, director, treballadors de departaments,...) per obtenir la resposta més precisa al tipus de qüestió que se'ls plantegi.

En principi, és recomanable que **aquestes enquestes siguin anònimes**, pel que no caldrà que s'incorporin les dades identificatives de la persona que proporciona la resposta, ja que el que realment ens interessa és la informació que ens pugui aportar.

Per mitjà d'aquestes entrevistes es podrà profunditzar en els punts de vista de cadascun d'aquests usuaris i la seva àrea de treball que afecten a nivell de seguretat informàtica.

A més, ajudaran a resoldre de forma més clara qüestions sobre aspectes que resultin més complexos o que no apareguin suficientment detallats a la documentació recollida prèviament. Per aconseguir el major detall possible, serà molt recomanable que **les preguntes es plantegin de forma que la resposta sigui oberta** i no es limitin a una resposta afirmativa/negativa.

Així mateix, el format de les entrevistes deuria permetre un millor coneixement de l'opinió dels empleats sobre les funcionalitats i l'equipament informàtic que utilitzen, amb la qual cosa s'aconsegueix **conèixer quines són les àrees més crítiques**, com també **descobrir possibles debilitats** i valorar si les polítiques de seguretat establertes són les més adequades.

Depenent del resultat obtingut d'aquestes entrevistes, l'auditor pot plantejar-se la necessitat de realitzar proves que en un primer moment no s'havien planificat.

El plantejament de les entrevistes seria el següent, diferenciat segons el càrrec dels membres de l'organització que ha de proporcionar la informació a l'auditor, ja que aquests proporcionaran la informació que permeti identificar deficiències en el nivell de seguretat informàtica existent, per a d'aquesta manera, elaborar les mesures de millora un cop estudiades:

Enquesta al Director de l'organització
•Es troba actualitzat i documentat el Pla de Seguretat Informàtica? •Qui és el responsable de la implantació de polítiques i procediments de seguretat de l'organització? •Com s'impulsen i quin seguiment se'n fa de les polítiques de seguretat dissenyades pel departament de sistemes per a que s'apliquin a tota l'organització? •Com s'acorden els plans de contingència i qualsevol activitat que contribueixi a la millora de la seguretat informàtica? •Es disposa d'un pla de manteniment integral dels sistemes d'informació? •Existeix un pla de comunicació per donar difusió a tot el personal sobre qualsevol procediment a seguir per millorar la seguretat informàtica? •Quines mesures de seguretat existeixen per protegir els equips del risc de furt, incendi, talls d'energia,...? •Qui avalua i proposa l'adquisició d'equips i mesures conduents a la seguretat informàtica dels actius i sistemes d'informació? •S'ha establert un procediment tant per l'entrada de nou personal com per les baixes dels empleats que marxen de l'organització? •Es programen informes per localitzar usuaris inactius del sistema que es poden deshabilitar? •Existeix un procediment disciplinari per incompliment de les mesures i de les polítiques de seguretat i privacitat de la informació? •Existeixen directrius a seguir per connectar nous equips a la xarxa? •Qui autoritza la publicació de nou contingut al lloc web i a la intranet de l'organització? •Existeix un responsable de la seguretat física de l'edifici? •Quins mitjans es fan servir per controlar els accessos físics (targetes de control d'accés, vigilants de seguretat, alarmes, tancaments amb clau,...? •S'enregistra d'alguna forma l'accés de les persones que accedeixen a instal·lacions on es localitzen equips de la infrastructura de xarxa? •Es controla el treball que s'ha de realitzar fora de l'horari habitual?

Taula 10. Enquesta al director de l'organització

Enquesta al personal Tècnic Informàtic
•En cas de detecció d'una vulnerabilitat o incident, quines són les accions per reduir els riscos? •Existeix un pla de seguretat informàtica per afrontar possibles incidències en relació a aquesta? Quins serien els punts principals sobre els que es recolza? •Com es gestiona la continuïtat del negoci davant d'un incident que podria produir la interrupció del servei? •A través de quines accions es protegeixen i recuperen els seus processos crítics contra els efectes d'un desastre en els sistemes d'informació? Aquestes accions estan procedimentades? •Quina és la periodicitat de l'actualització dels procediments relacionats amb la seguretat informàtica? •S'ha produït la caiguda del sistema per esgotament dels recursos o degut a un atac? En cas afirmatiu, amb quina freqüència es produeixen aquests incidents? •Quin és el circuit que es segueix per advertir d'un incident o de la vulnerabilitat detectats? •Les mesures incloses al pla de seguretat de l'organització són coherents amb la importància de la informació existent i els riscos que podria haver d'afrontar? •Quin tipus de mesures de seguretat existeix a la xarxa (xarxes perimetrals, criptografia,...)? •Es controla que les claus per autenticar-se als sistemes es modifiquin amb freqüència? •Quin grau de complexitat han de tenir les contrasenyes per considerar-se vàlides? •Com valora el nivell de seguretat de la infrastructura informàtica existent per protegir la xarxa de l'organització? Es pot considerar suficient o caldria implantar millores (de forma urgent, a mig termini,...)? •Quin és el nivell de seguretat a nivell de programari per protegir la xarxa de virus o d'atacs intrusius? •S'utilitza algun analitzador de xarxa per descobrir vulnerabilitats? Amb quina freqüència? •Es pot considerar que existeix una cultura de seguretat suficientment extesa entre tot el personal de l'organització? •Les llicències d'ús dels programes són vigents i compten amb les condicions exigides? •Es monitoritza el sistema per determinar si es compleixen les directrius establertes per la política de seguretat? •L'inventari d'actius s'actualitza sempre que hi ha un canvi? •Hi ha establertes unes directrius per gestionar els canvis periòdics dels recursos informàtics (per obsolescència, necessitats de l'organització,...)? •La ubicació on són els equips de xarxa es troba resguardada de desastres (com inundacions, sabotatges, incendis,...)? •Les instal·lacions on s'hostatgen els equips de xarxa són només accessibles a personal autoritzat?

Taula 11. Enquesta al personal Tècnic Informàtic

Enquesta als Usuaris
•S'ha enlentit, o fins i tot, s'ha hagut de suspendre l'atenció als usuaris o els clients perquè els sistemes d'informació o l'accés a la xarxa es trobaven inoperatius? •S'han produït incidents com la pèrdua d'informació, o fins i tot, la seva indisponibilitat ocasionada per un atac inesperat a les bases de dades? •Coneix el procediment per recuperar informació emmagatzemada a la xarxa? •Quin sistema utilitza per recordar les contrasenyes: disposa d'un aplicatiu gestor de contrasenyes, únicament les memoritza, o les anota en algun lloc? •En la seva opinió, caldria realitzar millores en seguretat als recursos informàtics? •Com que els equips de l'organització es connecten a Internet, s'han trobat amb la problemàtica de correus indesitjats (spam), arxius adjunts amb virus,...? •Coneix quin antivirus té instal·lat a l'equip i com utilitzar-lo per analitzar els fitxers o els dispositius d'emmagatzematge extern? •En quin estat es troba el tallafocs del seu equip informàtic (actiu/inactiu)? •Les credencials d'accés al sistema es canvien periòdicament, tant les que es fan servir per a la xarxa local com les xarxes inalàmbriques? •Aquestes claus d'accés són diferents per a cadascuna de les aplicacions i no guarden semblança amb paraules formades pel seu nom, dni, data de naixement,...? •De quina informació disposa sobre les polítiques de seguretat informàtica de l'organització? •Amb quina freqüència rep accions formatives per actualitzar els seus coneixements a nivell de seguretat informàtica? •Existeix algun procediment formal per utilitzar els equipaments informàtics i d'altres elements que formen part del sistema d'informació? •Com es controla el treball dels documents que contenen dades confidencials?

Taula 12. Enquesta als usuaris

5.2. Disseny dels checklists/qüestionaris

Els qüestionaris permetran enregistrar totes les deficiències i les evidències que es detectin durant l'auditoria. D'aquesta manera, es podrà analitzar la presència de riscos a cadascun dels elements esmentats al llarg de la seva estructura.

Per a la seva elaboració, es basaran en les normes ISO relacionades amb la seguretat informàtica i que s'han esmentat anteriorment.

Per altra banda, és recomanable realitzar preguntes equivalents redactades de forma diferent, a fi de poder descobrir possibles contradiccions.

Podem classificar els riscos que afronten els sistemes informàtics i de comunicacions depenent d'on recau la seva afectació, de forma que l'auditor desenvoluparia els següents qüestionaris:

Sobre la seguretat física i les infrastructures

- *Riscos naturals: com els produïts per agents atmosfèrics (huracans, pluja molt intensa,…), geològics (terratrèmols),…*

- Riscos tecnològics*: talls elèctrics, incendis elèctrics, avaries d'instal·lacions i centraletes, contaminació electromagnètica,…*

- *Riscos socials: desordres públics, actes terroristes,…*

Gestió de la continuïtat del negoci

- El sistema compta amb un pla de recuperació de desastres (DRP) en què estiguin definits els requeriments necessaris per permetre la continuació o la recuperació de les funcions més crítiques en cas d'interrupció no planificada?
- La planificació que permet la continuïtat del negoci en cas de desastre té actualitzats i documentats tots els processos i controls per gestionar-la?
- Es disposa d'equipament redundant destinat a garantir la continuïtat del servei en cas d'avaria o fallada d'algun dels seus components?
- Existeixen sistemes alternatius per poder transmetre la informació en cas d'incidència?
- Amb quina freqüència es revisa i es verifica l'eficàcia dels plans per assegurar la continuïtat de l'activitat en cas de desastre?

Polítiques de Seguretat de la Informació

- S'han elaborat documents en relació a les Polítiques de Seguretat de la Informació?
- En cas afirmatiu, aquests s'actualitzen periòdicament?
- S'ha donat difusió d'aquests documents i es té constància de la seva comprensió per part de tots els membres de l'organització?
- S'avisa amb suficient antelació a la Direcció de les tasques de manteniment que poden implicar un tall en el servei (per exemple, aturades degudes a comprovacions en els quadres elèctrics)? S'informa el temps estimat d'interrupció?
- Quin protocol es segueix per gestionar les vulnerabilitats tècniques (per exemple, si es produeix un tall elèctric)?

Seguretat física i ambiental

- En línies generals, de quins sistemes de protecció contra amenaces externes i ambientals es disposa?
- Existeix un pla de manteniment a l'edifici que inclogui actuacions tals com: simulacres de talls de llum, revisió del cablejat,…
- Hi ha equipaments instal·lats que evitin les incidències que se'n poden derivar de les descàrregues o talls elèctrics (ex. sistemes d'alimentació ininterrompuda (SAI)?
- Els quadres elèctrics es troben degudament etiquetats i protegits?
- Quina és la capacitat màxima del SAI per fer front a la tallada del subministrament elèctric (en hores)?
- Els sistemes es troben connectats a la fase de xarxa elèctrica de forma separada a la de la resta d'aparells que podrien sobrecarregar-la?
- Es compta amb sistemes d'extinció d'incendis adequat (columna seca, extintors degudament carregats i revisats)?
- De quin tipus d'extintors es disposa: manuals, automàtics,…?
- El personal ha rebut formació per manipular els extintors?
- Existeixen prohibicions com fumar, prendre aliments o utilitzar elements inflamables a les instal·lacions que contenen infraestructura informàtica crítica? En cas afirmatiu, es senyalitzen de forma visible aquestes prohibicions?
- Les dependències disposen de sistemes de prevenció d'incendis, com detectors de presència de fums?
- Els equips d'aire acondicionat de les instal·lacions amb equipament informàtic crític és redundant? Mantenen unes condicions de control d'humitat i temperatura adequades?
- El terra tècnic de les instal·lacions és registrable, ignífug i antiestàtic?
- Les preses de terra es troben degudament autoritzades?
- La instal·lació del cablejat de xarxa segueix la norma de cablejat estructurat?
- El cablejat de xarxa està apantallat com a mesura de protecció?
- Hi ha risc de contaminació per emissions electromagnètiques de forma que aquestes podrien ser captades per intrusos?
- Un cop impressos els documents, aquests són retirats per evitar l'accés a personal no autoritzat?
- De quina manera es controla l'accés de persones externes a l'organització? Existeixen registres de les seves hores d'entrada i sortida?
- Les àrees on s'ubiquen els equips principals de la xarxa es troben delimitades com zones d'accés restringit?
- Els racks de comunicacions es troben en llocs més aïllats de l'edifici? Quines són les mesures de seguretat física que els protegeixen d'accessos no autoritzats?
- Es realitza una neteja periòdica dels habitacles on s'ubiquen els racks de comunicacions i d'altres equipaments essencials de la xarxa informàtica?
- Com es controla el perímetre de seguretat física de les instal·lacions, oficines, àrees de càrrega,...? Aquestes compten amb sistemes de vigilància com poden ser les càmeres de seguretat?

- Es signen les sortides d'equipament informàtic de l'edifici?
- Existeix una política de permisos d'accés dels usuaris de l'organització a les aplicacions i la informació que hi circula?
- Es realitza una actualització periòdica de les contrasenyes d'accés al sistema?
- En cas que personal extern hagi de treballar amb els equips corporatius, quins permisos d'accés temporal se'ls donen?
- Els dispositius que reprodueixen documentació (multifuncions, impressores,...) es localitzen a àrees d'accés restringit? En cas contrari, quins sistemes de protecció dels documents es fan servir (per exemple, impressió sota contrasenya o targeta)?
- Es disposa d'equips destructors, com trituradores de paper i dispositius d'emmagatzematge d'informació, per eliminar de forma segura la documentació?
- Es xifren els dispositius d'emmagatzematge per a que la informació resulti il·legible en cas que s'extraviïn o siguin robats?
- En alguna ocasió s'ha divulgat informació de forma no autoritzada, fora de l'organització (per ex. per robatori d'aquesta), ja fos a través de personal extern o del propi d'aquesta?
- S'han implementat aplicacions per a la detecció d'intrusos (IDS) per monitoritzar els sistemes i tràfic de la xarxa per detectar atacs a la seva seguretat?
- S'han detectat accessos no autoritzats en alguna ocasió? Si és així, es va estudiar el motiu i de quina manera l'atacant va aconseguir l'accés?
- Hi ha instal·lats programes d'encriptació de dades als servidors per evitar que la informació emmagatzemada s'utilitzi en cas de robatori?

Classificació i control d'actius

- Existeix un inventari d'actius actualitzat per poder controlar la pèrdua o el robatori d'equips?
- S'ha realitzat una classificació d'aquests actius segons el grau de protecció que han de rebre i que vindrà donat per factors com el seu valor, criticitat,…?
- Segons aquesta classificació, s'han desenvolupat procediments per a l'ús d'aquests actius de forma adequada?
- Aquests actius es protegeixen en consonància amb el seu grau de protecció?
- S'actualitzen les sortides i entrades d'equipament als inventaris amb freqüència?
- Cadascun dels equips disposa d'una etiqueta amb un codi o referència que l'identifica de forma única?
- Qui proporciona l'autorització quan es demana reubicar o retirar maquinari dins de l'organització?
- S'ha establert un procediment per assegurar que els equips retirats siguin formatejats abans que siguin reutilitzats?
- Els equips compten amb la protecció necessària per evitar una possible manipulació o un ús indegut mentre els seus usuaris no es troben presents?

Taula 13. Qüestionari sobre riscos en la seguretat física i les infrastructures

Sobre la seguretat lògica

Són aquells riscos relacionats amb la tecnologia, com poden ser els ocasionats per avaries en l'equipament informàtic o pel funcionament incorrecte de programes de protecció. Aquests riscos van en augment: suplantació d'identitat, l'entrada de virus o d'altre programari indesitjat, espionatge industrial, fuites d'informació,...
Els danys poden ser sobre els encaminadors de la xarxa, produir interrupcions del servei, afectacions de diversa gravetat per la pèrdua d'informació ubicada a unitats de xarxa o als propis equips dels usuaris,...

Gestió de l'operació i les comunicacions

- Com es realitzen els controls a la xarxa per analitzar el tràfic d'informació que hi circula?
- En cas d'incident lògic, s'estudien les causes per prendre mesures que protegeixin de nous incidents similars?
- Quins mecanismes s'utilitzen per proporcionar major seguretat als serveis en xarxa davant d'atacs (per exemple, atacs de denegació de servei o DoS)?
- Amb quina periodicitat s'actualitzen les llicències dels antivirus? I les aplicacions corporatives i les solucions ofimàtiques?
- Tots els equips i sistemes informàtics tenen instal·lat un antivirus actualitzat amb les darreres signatures de programari maliciós[24], és d'execució automàtica i la llicència és activa?
- Un usuari sense privilegis d'administrador pot desactivar l'antivirus?
- L'abast de l'antivirus el fa suficientment efectiu (és a dir, s'inclouen funcionalitats com l'anàlisi de pàgines web, correu electrònic,...)?
- Es realitza un registre i seguiment regular dels logs per detectar qualsevol comportament estrany en el sistema?
- Quines són les aplicacions i els serveis identificats com a crítics?
- Hi ha establert un pla de recuperació de la informació (programes, dades, configuracions,...) en cas de produïr-se un incident?
- S'ha definit quina és la informació prioritària que s'ha de reconstruir en cas de pèrdua?
- La programació de les còpies de seguretat inclou còpies completes o incrementals?
- Es documenta el procés de realització i restauració de còpies?
- Quin és el procediment a seguir per a la recuperació d'informació en cas de pèrdua?
- Quina és la freqüència amb la que es realitzen proves de recuperació per garantir la confiabilitat d'aquest procediment?

[24] Decálogo ciberseguridad empresas. Una guía de aproximación para el empresario [en línia]. [Consulta:]. <https://www.incibe.es/protege-tu-empresa/guias/decalogo-ciberseguridad-empresas-guia-aproximacion-el-empresario>

- Com es gestiona la seguretat de la xarxa per protegir els seus sistemes, aplicacions i la informació que hi circula?
- S'han establert directrius per a la transferència segura de la informació?
- En cas d'utilitzar serveis al núvol, s'han estudiat prèviament les condicions d'ús (confidencialitat de la informació, disponibilitat,...)?
- Els serveis del núvol permeten xifrar la informació abans de pujar-la per evitar un accés indegut?
- S'han definit procediments per efectuar un adequat control de la informació que s'intercanvia amb altres organitzacions?

Seguretat i personal

- Existeix un procediment per autoritzar la instal·lació de programari no relacionat amb les activitats de l'organització?
- L'àrea de sistemes és sempre l'encarregada de realitzar la instal·lació dels programes?
- Com es realitza la notificació dels successos detectats que poden afectar a la seguretat de l'informació? Els empleats estan conscienciats de la necessitat de comunicar-los per tal de reduir el seu impacte i solucionar els danys que se'n derivessin?
- Quin protocol han de seguir els empleats davant la presència d'un virus? Tothom coneix aquest protocol?

Seguretat organitzacional

- Com s'han definit les responsabilitats per a la seguretat de la informació?
- Es realitzen reunions de coordinació de la seguretat informàtica?
- Quines mesures es prenen per des de la Direcció per donar suport a les iniciatives de seguretat?
- Els empleats nous que s'incorporen signen compromisos de confidencialitat?
- Quins són els punts bàsics dels acords de confidencialitat i secret que signen les persones, ja sigui perquè són clients, proveïdors o empleats de l'organització?
- S'han establert procediments disciplinaris per als empleats que cometen infraccions en relació a la seguretat dels sistemes i la informació?
- Hi ha contacte amb grups d'interés especial i/o associacions professionals especialitzades en seguretat informàtica?
- S'han desenvolupat polítiques i mesures de seguretat per protegir la informació que és tractada des d'equips mòbils i de teletreball?

Control d'accés

- Existeix una política de control d'accés als sistemes i aplicacions corporatives?

- En quins actius i sistemes s'han implementat mesures de control d'accés? En què consisteixen? - En funció del lloc de treball o de les tasques que desenvolupen els empleats, s'han definit diferents nivells d'accés als sistemes? - Quines restriccions s'estableixen en l'accés a la informació? Es revisen els privilegis d'accés dels usuaris? - Existeix un registre d'usuaris per assignar els permisos corresponents? - Qui activa els permisos d'accés i a qui els proporciona? - Amb quina freqüència es revisen els drets d'accés dels usuaris dels sistemes d'informació a fi de cancel·lar aquests drets un cop marxin de l'organització? - S'ha limitat l'accés al codi font dels programes únicament a aquells empleats que s'encarreguen del seu desenvolupament? - En cas d'administrar remotament els equips connectats en xarxa, amb quin mecanisme de control d'accés segur es compta que permeti a l'usuari autoritzar aquest accés? - S'utilitzen elements per controlar l'amplada de banda i impedir l'accés a certs llocs web? - La connexió a la xarxa dels equips es troba distribuïda en diferents VLAN's depenent dels departaments o àrees a que pertanyin? - Com es controla l'accés a la xarxa corporativa des d'equips mòbils i de teletreball? - Es realitza un monitoreig per detectar accessos indeguts a la xarxa o als servidors?
Relacions amb els proveïdors
- S'ha elaborat una política de seguretat de la informació acordada amb els proveïdors que han d'accedir als actius de l'organització per reduir els riscos que suposa aquest accés? - En cas afirmatiu, quins requeriments de seguretat s'han establert amb els proveïdors en funció de les tasques que tenen encarregades (substitució de components, emmagatzematge,…)? - Els contractes signats amb els proveïdors del núvol o els que proporcionen altres serveis pels quals poden tenir accés a dades personals especialment protegides, contemplen el tractament d'aquestes dades atenent al RGPD? - Els contractes amb els proveïdors estableixen les seves responsabilitats pel que fa a la seguretat de la informació que tracten, especialment aquella de tipus confidencial? - De quina forma s'audita o es revisa la prestació dels serveis dels proveïdors per assegurar que es manté el nivell acordat de servei? Amb quina regularitat es realitza el seu seguiment?

Taula 14. Qüestionari sobre riscos en la seguretat lògica

Sobre la seguretat tècnica integral

Són danys originats degut a un manteniment incorrecte, un mal ús, perquè no es renoven convenientment els equips, no existeix una comunicació efectiva dels incidents,…

Desenvolupament i manteniment de sistemes

- Quins procediments d'actualització o control de canvis en els sistemes, tant a a nivell de maquinari com de programari, s'han documentat?
- Aquests procediments inclouen els requeriments de seguretat de la informació que s'han d'incloure tant als nous sistemes com als ja existents?
- S'apliquen els pegats i les actualitzacions recomanades pels fabricants a fi d'evitar riscos de seguretat?
- S'utilitzen mecanismes de seguretat que evitin que se'n faci un mal ús dels sistemes?
- S'analitza la capacitat dels servidors a través de la seva monitorització periòdica?
- Hi ha contractats serveis de manteniment preventiu? Si és així, amb quina freqüència es realitza?
- En el cas del manteniment correctiu, quin és el termini d'actuació per part de l'empresa proveïdora per solucionar la incidència?
- Es compta amb un manteniment ampliat de 24 hores?
- Els reports de manteniment contenen dades essencials sobre l'equip reparat: data de la reparació, referència o número d'inventari de l'equip, número de sèrie, descripció de la tasca realitzada?
- Es disposa d'un calendari per a la renovació periòdica tant de l'equipament informàtic dels usuaris com del que compon la infraestructura de xarxa?
- Abans de la seva adquisició, s'estudia que l'equipament a renovar resulti compatible entre sí?
- L'equipament que es renova o els suports físics en desús que contenen informació, són formatejats prèviament abans de la seva retirada de l'organització? Si no és així, hi ha una empresa certificada que s'encarregui de la seva destrucció o esborrat segur?
- En quines condicions d'ordre es troben els equips que es fan servir a les instal·lacions de l'organització (hi ha desorganització, es mesclen equips en bon estat amb altres que no funcionen adequadament, hi ha dispositius o qualsevol altre material amuntegat,...)?
- S'elaboren informes sobre el desenvolupament dels projectes en execució dels sistemes d'informació?
- En cas que el desenvolupament del programari s'hagi contractat a una empresa externa, quina supervisió se'n fa de la seva activitat?
- Està procedimentat el procés d'implementació de canvis per efectuar un correcte control del canvi (criteris, requeriments tècnics, programes d'assaig,…)?

- Es realitzen proves prèviament a la implantació o pas a producció d'una solució informàtica?
- Es revisa tot el que implica el pas a producció de nous sistemes i aplicacions (requeriments de seguretat, rendiment i capacitat; aplicació de pegats i actualitzacions, acords de nivell de servei)?
- Es realitzen proves d'acceptació o tècniques després dels canvis per detectar possibles vulnerabilitats en els programes o que no hi ha afectació en les operacions de l'organització?

Seguretat i personal

- El personal coneix els procediments per comunicar qualsevol incident de seguretat o el funcionament incorrecte d'un sistema?
- Es proporciona als treballadors una formació adequada en l'ús de les eines informàtiques que faran servir a diari?
- Amb quina freqüència es convoca als empleats per a realitzar formacions o jornades de sensibilització en seguretat informàtica? La seva assistència és obligatòria o voluntària?
- Els empleats tenen accés a manuals de seguretat de la informació i de contingències per saber com actuar davant desastres?

Control d'accés

- Es controla que només el personal autoritzat pugui manipular el maquinari?
- S'ha documentat la política de control d'accessos autoritzats?
- Quin és el procediment a seguir per demanar l'accés a un determinat tipus d'informació? Es realitza a través d'un formulari signat, un aplicatiu d'incidències,…?
- Existeix un servei de directori (com pot ser *Active Directory*) per centralitzar i administrar els usuaris, amb polítiques de seguretat i restriccions?
- L'assignació dels permisos als usuaris es realitza de forma individualitzada o per perfils?
- Les contrasenyes per defecte de l'usuari administrador amb les que arriben els nous dispositius informàtics es modifiquen per evitar accessos indeguts a la seva configuració?
- S'enregistren els motius pels quals es modifica la contrasenya abans de caducar el termini en què es demana el canvi?
- Les contrasenyes assignades per primer cop als empleats requereixen que aquests es canviïn abans de començar a treballar amb el sistema autoritzat?
- L'autenticació dels usuaris inclou el doble factor d'autenticació (targetes de coordenades, claus enviades a un mòbil,…)?
- S'utilitza algun programari centralitzat per gestionar les contrasenyes?
- Quines polítiques restrictives de tallafocs s'han definit?
- Tots els equips de l'organització tenen activat el tallafocs de seguretat perimetral i d'aplicacions?

Compliment amb el marc jurídic

- Quines són les normes per les que es regeixen els procediments i protocols documentats en quant a les activitats conduents cap a la millora de la seguretat informàtica de cadascun dels diferents sistemes i actius d'informació?
- Es troben documentats i actualitzats els requeriments legals per donar-ne difusió entre els membres de l'organització?
- S'han establert les responsabilitats i els protocols que garanteixin la protecció i la confidencialitat de les dades personals? S'han basat en la legislació vigent?
- Quines mesures s'han adoptat per evitar l'ús de la informació amb finalitats diferents per a les quals es va recollir?
- S'afegeixen clàusules als correus electrònics informant de la privacitat de les dades incloses?
- S'ha establert un procediment per al tractament dels registres i la informació de l'organització d'acord amb els requeriments contractuals i legislatius (contra accessos no autoritzats, destrucció, falsificació,…)?
- Qui s'encarrega del compliment i la implementació de les polítiques i normes de seguretat de la informació?
- Quins procediments s'han implementat per complir amb els drets de propietat intel·lectual i d'ús del programari amb llicència?
- Amb quina freqüència es revisa el compliment de la normativa i dels estàndards de seguretat informàtica?

Gestió de l'operació i les comunicacions

- L'ús dels comptes de correu facilitats als empleats es destina exclussivament a activitats corporatives i no a fins personals?
- S'extremen les precaucions quan els missatges de correu incorporen enllaços o arxius adjunts? Quines mesures es prenen en tal cas?
- Els correus electrònics que contenen dades confidencials són encriptats?
- Els missatges de correu enviats per l'organització respecten el format d'imatge corporativa?
- Els racks es troben degudament etiquetats i el seu cablejat es troba documentat per localitzar més ràpidament els problemes de la xarxa?
- Com s'evita o es restringeix d'alguna forma la navegació per pàgines que representen una entrada potencial d'amenaces: pàgines de descàrregues, xarxes socials, jocs online,…?
- Quines precaucions es prenen en l'ús de dispositius extraïbles en el cas que el seu ús estigui permès (llapis de memòria, discs durs externs,…)?
- Els usuaris connecten dispositius externs (memòries, discs externs,…) als equips corporatius? Si és així, com comproven l'existència de virus en aquests?

- Quan l'empleat s'absenta del seu lloc de treball, encara que sigui per un temps mínim, bloqueja la pantalla del dispositiu que fa servir? - Existeixen ports que sense estar en ús, estiguin oberts? Si és així, quins són i per quina raó es mantenen en aquest estat? - Es monitoritzen els ports oberts que ho són per necessitat? - Les còpies de seguretat estan programades per a que s'executin en períodes del dia en que no es desenvolupi activitat? - Els punts d'accés Wifi s'apaguen quan no es troben en ús per tal d'evitar el risc d'atacs innecessaris? - S'oculta la publicació del nom de xarxa SSID de les xarxes Wifi? - El senyal de la xarxa inalàmbrica es pot filtrar fora de l'edifici? - Quins protocols de xifrat segurs fan servir les connexions Wifi (WAP PSK,...)? - S'utilitzen claus suficientment complexes com per assegurar una major robustesa? Amb quina freqüència es demana el seu canvi? - En cas que els treballadors de l'organització desenvolupin tasques sota la modalitat de teletreball, quin protocol existeix i, en línies generals, en què consisteix?
Gestió dels incidents de seguretat de la informació
- S'ha creat un procediment per gestionar una resposta àgil i eficaç als incidents de seguretat? - Els proveïdors i els empleats de l'organització han estat conscienciats de l'importància de comunicar qualsevol vulnerabilitat o debilitat que afecti a la seguretat de la informació? - Existeixen diferents canals per comunicar a tots els membres de l'organització els incidents de la forma més ràpida possible? - En cas d'incident, ja sigui físic o lògic, s'estudien les causes per prendre mesures que protegeixin de possibles incidents similars en el futur? - Els incidents de seguretat són avaluats per classificar-los segons la seva importància i gestionar-los atenent a la seva importància? - Com es centralitza la comunicació dels incidents de seguretat, ja sigui per difondre informació o per rebre notificacions al respecte?

Taula 15. Qüestionari sobre riscos en la seguretat tècnica integral

5.3. Proves tècniques

Normalment, el desenvolupament dels atacs s'efectua a través de diferents etapes. Aquestes es poden resumir en les següents:

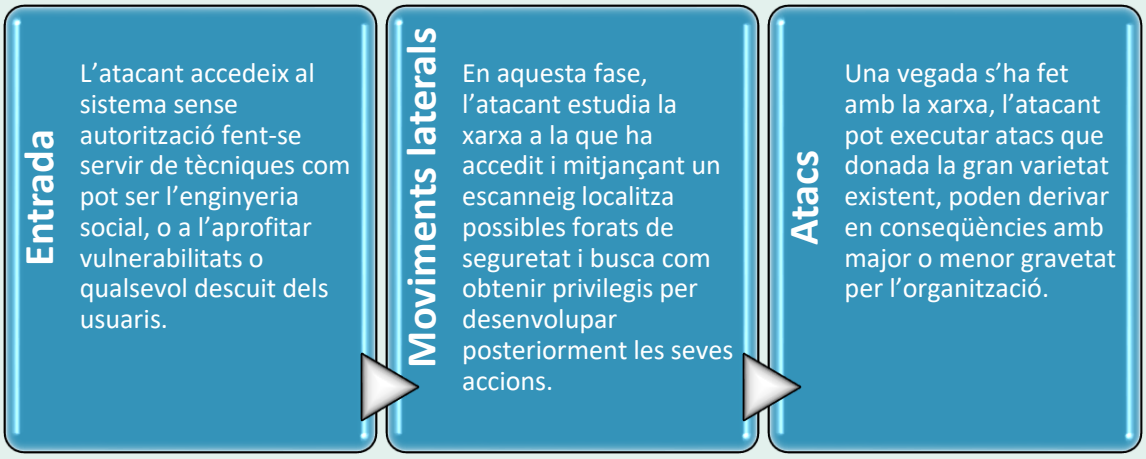


Figura 14. Etapes d'un atac

Per tot això, és convenient que l'auditor imagini **possibles escenaris d'actuació d'un atacant** a l'hora de dissenyar les proves per demostrar si alguna de les fases anteriors és assolible per demostrar que existeix un risc.
A més, caldrà tenir en compte que **l'entorn a auditar pot ser diferent**. Així, per exemple, un Departament de Qualitat tindrà uns perfils d'usuari, configuracions de programari, estructura organitzativa,... diferents als d'un Departament de Recursos Humans.
Tanmateix, l'elaboració de les revisions s'ha de realitzar de forma que **la seva execució no posi en risc l'operativitat** de l'organització o dels seus serveis més crítics. És per això, que a banda del procediment a seguir per desenvolupar les proves, és important l'establiment d'un pla de comunicació abans de començar-les per fixar, si fos necessari, en quin moment s'han de detenir i quan es poden proseguir.

Per això, a l'hora de planificar les proves caldrà realitzar les següents activitats:

- **Dissenyar quines seran les revisions i les proves a efectuar**: per tal de no allargar innecessàriament el temps d'auditoria interna, cal tenir en compte que si anteriorment a aquesta s'han realitzat d'altres auditories que incloïen les mateixes proves, aquestes es poden anul·lar. Però això, sempre i quan no s'hagin modificat les mesures de seguretat per dur a terme mesures correctores recomanades per l'auditoria efectuada o per accions de millora contínua.
  A més, les proves s'hauran de desenvolupar atenent als sistemes d'informació que es trobin més exposats i el perfil de riscos de l'organització, contemplant els possibles escenaris d'un atac o les vies de què pot disposar l'atacant per poder executar-lo.

- **Detallar en què consisteix cada prova:** amb tots aquells aspectes que són d'interés de l'auditor per a la seva execució òptima, d'entre els quals es contemplarien:
  - si caldrà la presència o inclús la col·laboració d'algun usuari o dels professionals informàtics de l'organització, o si pel contrari, l'auditor la desenvoluparà de forma autònoma;
  - establir l'horari d'inici i de finalització de cadascuna de les revisions;

- decidir la conveniència de realitzar la prova dins d'un interval de temps de major o menor càrrega del sistema;
- si per la tipologia de la prova, en cas que sigui possible, és més convenient realitzar-la fora de l'hora de treball dels empleats per no destorbar la seva tasca,…

- **Enumerar els recursos o eines per executar les comprovacions**: en alguns casos es podran realitzar en els mateixos equips, per observació directa o mitjançant simulacions de situacions que es podrien donar, com podrien ser les següents:
  - Backup d'una còpia de seguretat: es pot realitzar una prova de recuperació d'informació per comprovar que el sistema de còpies de seguretat funciona correctament i pot respondre davant un desastre de pèrdua d'informació. Amb aquesta finalitat, per realitzar la prova, es pot fer servir el mateix programari que utilitza l'organització per executar les còpies de seguretat.
  - En cas que l'organització disposi de xarxa Wifi, de la mateixa manera que amb els sistemes connectats per mitjà de cablejat, caldrà analitzar els equips que en donen accés: el maquinari que fa servir, el tipus de xifrat i contrasenyes utilitzades, identificar el SSID i comprovar la potència del senyal.

  Però bona part de les proves també requerirà d'algun recurs extra com poden ser un equip portàtil i el corresponent programari específic:

  - *Nmap*: com a eina que permet explorar la xarxa, a l'auditoria s'utilitzarà per realitzar comprovacions d'aquesta, resultant molt útil pel descobriment de vulnerabilitats, serveis en execució i ports oberts innecesàriament que poden posar en risc la disponibilitat, integritat i confidencialitat de la informació que circula per l'empresa.
    La importància d'aquesta revisió permet descobrir aquells serveis o ports que són una porta d'accés de virus troians i atacants als que permeten accedir com si fossin empleats de l'organització per poder controlar remotament el sistema i explotar les seves vulnerabilitats. Així mateix, a través d'aquesta eina es pot determinar quins servidors i equips informàtics es troben en xarxa, el seu sistema operatiu i les característiques d'aquest maquinari. Amb aquesta finalitat, una de les ordres que resultarà més útil per l'auditor a l'hora d'executar les proves serà '*nmap -PN -sT –Sv*'[25] per poder mostrar tant els ports oberts com els tancats, la seva identificació i els serveis que s'executen en ells.

    SQLmap és altre detector molt interessant que pot fer servir l'auditor per localitzar vulnerabilitats en multitud de motors de bases de dades (MySQL, Oracle, H2, Informix, entre d'altres) i a les pàgines web corporatives.

[25] Castillo, A., Hidalgo, J. & Guano, C. (Julio - diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

WPScan també s'utilitza per escannejar els llocs web per localitzar els plugins que poden ser explotats pels atacants, així com per identificar si les contrasenyes són dèbils, de forma que contribueix a recomanar als usuaris que incrementin la fortalesa d'aquestes, renovant-les per altres de major complexitat.

Altre solució per localitzar vulnerabilitats és *Nessus*, que com els anteriors, s'utilitza per escannejar els serveis web. Però també permet detectar entre d'altres, aquelles que poden originar atacs deguts a la manca de pegats de seguretat o una configuració de seguretat incorrecta del sistema, els del tipus "Man in the middle" que podrien exposar dades sensibles de l'organització, i inclús els que poden afectar a dispositius mòbils.

- *WireShark*[26]: Aquest analitzador de la xarxa permetrà realitzar la captura de paquets d'informació en temps real, de forma que proporciona a l'auditor diferent informació molt detallada sobre els equips de la xarxa: detecció de les versions dels seus sistemes operatius, el rang i subrangs de la xarxa, els equips que es troben actius, qui o quins serveis s'estan fent servir en el moment que es realitza l'anàlisi i quins d'ells utilitzen major volum de l'amplada de banda,…
  Un dels avantatges que proporciona aquest analitzador és la seva capacitat per identificar més d'un miler de protocols, inclòs el *Wireless* i no únicament aquells de xarxa cableada, pel que permet conèixer com funciona la xarxa per mitjà del registre de les activitats que s'hi generen.

  Per mitjà d'aquesta eina, l'auditor pot detectar connexions amagades d'un codi maliciós amb adreces remotes amb l'intenció d'accedir a informació de la xarxa, o analitzar el seu rendiment en diferents invervals horaris, de forma que contribueix al disseny d'aquelles decisions que siguin més adequades per afrontar aquestes anomalies. Així mateix, també permet comprovar l'existència de certes pràctiques poc recomanades dins d'una xarxa empresarial, com pot ser la descàrrega de fitxers multimèdia que no estan relacionats amb les tasques laborals i que redueixen l'amplada de banda, el que pot originar la saturació de la xarxa, i per tant, un risc d'indisponibilitat de la informació.

  A més, és una eina amb la que es poden treballar fàcilment els resultats obtinguts, ja que aquests es poden exportar i guardar, generar gràfics o

[26] *Análisis de una red en un entorno IPV6: una mirada desde las intrusiones de red y el modelo tcp/ip*. Universidad Francisco de Paula Santander Ocaña. Colombia: Revista Colombiana de Tecnologías de Avanzada, 2017-, vol. 1, núm. 29. ISSN: 1692-7257

estadístiques entre d'altres formes per visualitzar-los[27], per tal de facilitar la seva anàlisi.

En definitiva, mitjançant aquesta eina es poden detectar errors i vulnerabilitats que suposen una amenaça pels sistemes, reduïnt els danys que aquests podrien provocar.

Mentre que altres comprovacions requeriran **l'observació de l'auditor**, com pot ser la visualització dels registres logs o de les configuracions dels equips.

En tot cas, **les mostres obtingudes a partir de les proves tècniques, han de ser clarament representatives**, per a que les conclusions obtingudes a partir d'elles siguin prou fidels a la realitat. Si no fos així, es pot decidir la creació de més mostres per assegurar que són suficients per a l'obtenció de resultats objectius.

Una vegada realitzades les proves, és molt important **documentar-les per a que serveixin com a evidència**, pel que pot ser útil la realització de fotografies, les còpies de registres o la creació de documentació en suport paper o electrònic, segons escaigui. Els resultats de cadascuna d'aquestes proves poden quedar reflexats mitjançant el següent model de documentació, que ha d'incloure sobre quin element es realitza la prova, en què consisteix aquesta i els recursos necessaris per realitzar-la (programari, equipament informàtic,…), així com el temps necessari i les possibles vulnerabilitats detectades:

Proves tècniques					
Organització: _____ Auditor: _____ Departament: _____ Data: _____					
Actiu auditat	*Descripció de la prova*	*Recursos implicats*	*Data d'inici*	*Data de finalització*	*Vulnerabilitats*

Taula 16. Taula amb el detall de les proves tècniques

A continuació, s'enumeren alguns dels aspectes sobre els que l'auditor hauria de realitzar les **avaluacions tècniques per tal d'identificar els riscos** de seguretat referents a:

[27] Análisis y captura de paquetes de datos en una red mediante la herramienta Wireshark [en línia]. [Consulta: 24 de novembre de 2022]. <http://repositorio.uisrael.edu.ec/bitstream/47000/168/1/UISRAEL-EC-SIS-378.242-404.pdf>

✓ Accés a la xarxa i gestió dels comptes per evitar el seu haqueig ✓ Configuració dels aplicatius, bases de dades i sistemes operatius per detectar deficiències o vulnerabilitats que facilitin intrusions perilloses ✓ Estudi de possibles escenaris de pèrdua d'informació ✓ Procediment de parxeig dels equips en xarxa ✓ Mesures de protecció de les connexions VPN ✓ Monitoreig de vulnerabilitats (ports innecessaris oberts,…) ✓ Revisió de la configuració de dispositius de xarxa (encaminadors, tallafocs,…) ✓ Revisió de codi de les aplicacions. ✓ Comprovació de la configuració de la WIFI (vulnerabilitats, accés,…)

Taula 17. Aspectes a avaluar per a la identificació de riscos

Atenent a les diferents etapes d'un atac es poden aplicar diferents tipus de proves:

Proves d'entrada

- Aplicació de tècniques d'enginyeria social diverses:
  *correus electrònics i pàgines web que simulen programari maliciós en el lloc dels empleats per obtenir dades i credencials.
  * correus electrònics que adjunten fitxers per simular programari maliciós.
  *introducció d'USB amb programari maliciós per realitzar simulacions.
- Accés anònim a la xarxa wifi per:
  *analitzar el tràfic i localitzar els sistemes connectats.
  *per obtenir credencials dels empleats.
  *per a l'execució de programari maliciós.

Proves de moviment laterals

- Reconeixement d'equips de treball d'empleats amb diferents perfils d'usuari.
- Realització d'una revisió de la xarxa de l'organització des d':
  *un equip d'un empleat.
  *una xarxa de tercers.
- Execució de controls d'un equip d'un empleat des de la xarxa Internet:
  *utilitzant un dispositiu físic.
  *per mitjà de programari maliciós.

Proves d'atac
• Accedir remotament a equips dels empleats. • Extreure informació continguda a la xarxa interna. • Estudiar escenaris d'intrusió a diferent equipament informàtic (servidors, encaminadors,…) • Accedir a informació estratègica o que pertanyi a clients, proveïdors,… de l'organització.

Taula 18. Proves per cadascuna de les etapes d'un atac

5.4. Proves d'observació de l'entorn

Aquesta observació directa permet verificar tot el que succeeix en l'organització, pel que l'auditor es troba en una situació real que li proporciona la visió que necessita al permetre-li investigar si es compleixen les mesures de seguretat contingudes als plans de seguretat o analitzar quines s'haurien d'incorporar.

Per a l'observació de l'entorn on es desenvolupa l'activitat, **es determinarà quines són les instal·lacions, àrees o departaments de l'empresa que cal visitar** per poder examinar l'estat en que aquestes es troben i els diversos equips informàtics que s'ubiquen, tant el que pertany a la infrastructura informàtica pròpiament dita, com l'utilitzat en l'activitat diària de l'empresa:

- condicions ambientals (ventilació, iluminació,...),
- ordre i neteja,
- la seguretat dels accessos físics (portes amb clau, videovigilància,...),
- com es realitzen els processos i l'operativa diària dels treballadors,...

Així, per exemple, s'inspeccionarà si les instal·lacions del cablejat de xarxa compleixen amb la normativa del cablejat estructurat, com són els estàndards ANSI/EIA/TIA-568[28] o la norma EN 50173-1.

[28] Standards ANSI/TIA/EIA 568-B Commercial Building Telecommunications Cabling Standard [en línia]. [Consulta: 29 de novembre de 2022].
<https://www.bing.com/ck/a?!&&p=9733e060c3be32f4JmltdHM9MTY2OTc2NjQwMCZpZ3VpZD0zNjZmMWU3Ni1mNzM1LTZjMjUtMzYwYi0wYzFhZjY3YzZkMDYmaW5zaWQ9NTE5OA&ptn=3&hsh=3&fclid=366f1e76-f735-6c25-360b-0c1af67c6d06&psq=ANSI%2fEIA%2fTIA-568&u=a1aHR0cHM6Ly93d3cuY3NkLnVvYy5nci9-aHk0MzUvbWF0ZXJpYWwvQ2FibGluZyUyMFN0YW5kYXJkJTIwLSUyMEFOU0ktVElBLUVJQSUyMDU2OCUyMEIlMjAtJTIwQ29tbWVyY2lhbCUyMEJ1aWxkaW5nJTIwVGVsZWNvbW11bmljYXRpb25zJTIwQ2FibGluZyUyMFN0YW5kYXJkLnBkZg&ntb=F>

Per tant, entre d'altres, caldrà revisar si a les ubicacions on es troben els racks de veu i dades no hi ha brutícia o presència de materials que puguin afavorir incendis, com també que aquests presentin un parxeig ordenat i ben organitzat.

A l'hora de documentar aquestes proves d'observació, l'auditor intern haurà d'**especificar tant l'actiu comprovat com la data** en què va tenir lloc l'observació i la seva **ubicació exacta** (lloc de l'edifici, departament al que pertany, usuaris als que afecta,...)

En tot cas, l'auditor tindrà present que pot mancar alguna mesura de seguretat, però estudiarà d'altres que actuïn com substitutes, valorant si proporcionen la mateixa efectivitat que aquella de la qual s'ha detectat la seva mancança.

5.5. Revisió de la documentació

Cal revisar tota la documentació existent que pugui facilitar informació completa que resulti útil per a millorar la seguretat informàtica. Per tant, es pot comptar amb els següents documents, en els quals han de constar les dates de la darrera actualització:
- **inventaris de maquinari,**
- **inventaris de programari**.

Però també cal incloure tota aquella referent als **plans i polítiques** (de seguretat, contingència,...), els **procediments de treball** relacionats amb la seguretat dels sistemes informàtics, com també els **contractes** (de manteniment preventiu, correctiu,...), juntament amb d'altres que han estat enumerats a l'anterior apartat *4.4.2.1 Instruments de recol·lecció de la informació per l'auditoria interna.*

En el cas de la Política de Seguretat, per a que el document que la descriu compleixi amb els requeriments de la norma UNE-ISO/IEC 27001 i sigui realment útil per a l'organització, l'auditor intern haurà de tenir en compte els següents aspectes:

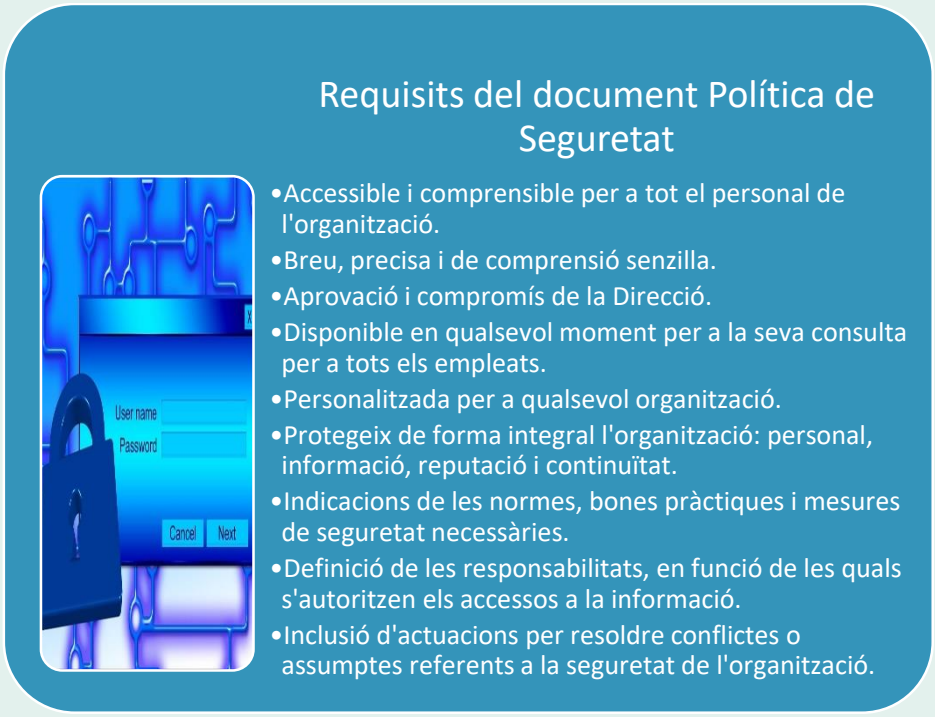


Figura 15. Requisits del document de la Política de Seguretat segons la norma UNE-ISO/IEC 27001

Tot i que deuria ser un fet excepcional, pot succeir que l'auditor, per alguna raó, tingui restringit l'accés a determinats documents o elements que es deurien haver incorporat en el procés, pel que ho farà constar a l'informe d'auditoria, indicant si aquesta circumstància ha pogut influir a les conclusions definitives. A més, l'auditor ha de sol·licitar que es realitzi una comunicació per escrit fent referència a aquesta limitació d'accés i la seva justificació.

5.6. Anàlisi de riscos

A partir de l'execució de les anteriors tasques, com són els checklists, les conclusions obtingudes a través de la documentació recollida, l'observació de l'entorn, l'estudi dels actius informàtics,... **s'identifiquen les vulnerabilitats i les amenaces, així com l'impacte** que aquestes poden suposar per a la seguretat informàtica de les àrees auditades.

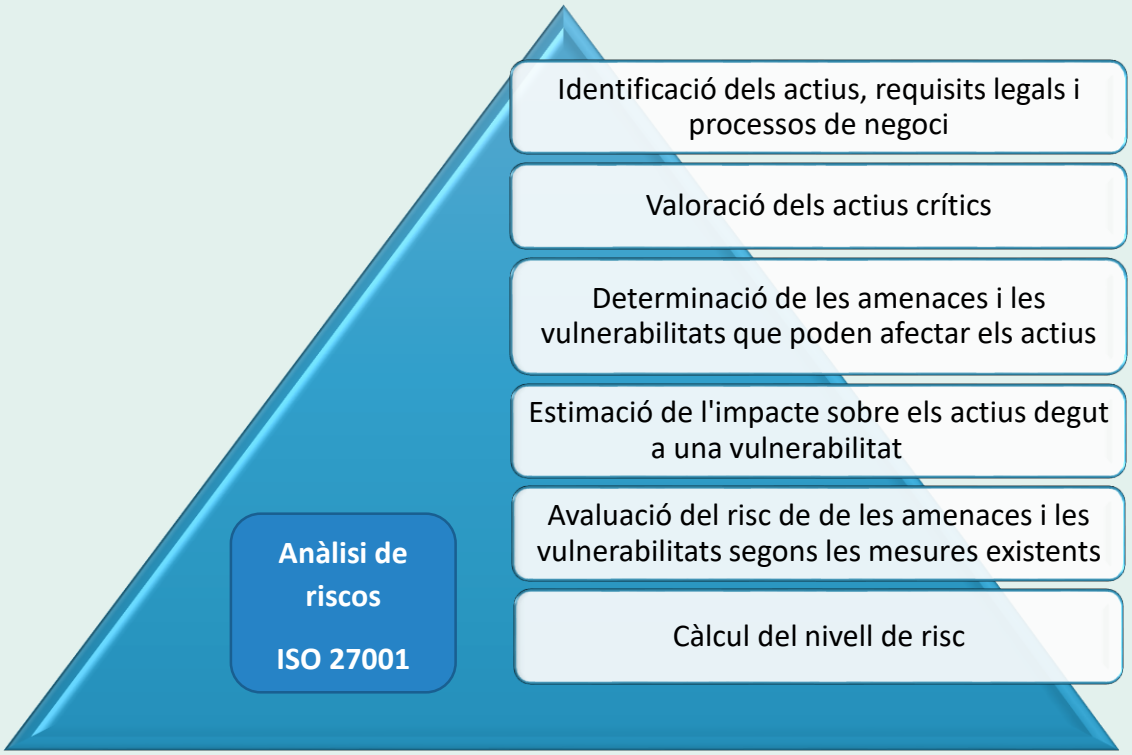


Figura 16. Etapes de l'anàsisi de riscos segons la norma UNE-ISO/IEC 27001

A través d'aquesta anàlisi es disposarà d'informació per **gestionar els riscos a través de la implementació de les salvaguardes i els controls necessaris** que redueixin el seu impacte i la seva probabilitat en el futur.

Aquesta **avaluació dels riscos**, que ha de quedar enregistrada, ha de considerar els objectius de la política de seguretat, les necessitats dels usuaris (disponibilitat, integritat,...), aportar informació vàlida i completa, i complir amb els requeriments legals, com pot ser evitar la propagació d'informació referent a dades personals a empleats no autoritzats.

Per prevenir els riscos que es podrien produir en el futur o afrontar aquells que ja s'estan produïnt es poden dur a terme diferents accions:

Figura 17. Accions a prendre davant dels riscos

Així mateix, cal tenir en compte que, tant l'anàlisi com la gestió dels riscos, són processos que cal actualitzar regularment.

6. Finalització de l'auditoria

6.1. Elaboració i entrega de l'informe final amb els resultats obtinguts

Al finalitzar l'auditoria, s'elabora un primer **informe provisional** que es discutirà amb la Direcció. Una vegada creat, es distribueix **l'informe definitiu** que posteriorment s'haurà preparat amb els resultats obtinguts de les revisions i les proves efectuades durant tot el procés auditor al Responsable de Seguretat Informàtica i a la Direcció.

Per tal que sigui comprensible als directors o tercers de l'organització és convenient que no inclogui termes o acrònims tècnics, o en cas que això no sigui possible, convindria destinar un annex del document a explicar el significat d'aquests conceptes de forma clara.

En aquest informe s'inclourà un llistat amb tots aquells **aspectes de millora** que s'han detectat, especificant sobre quins cal actuar amb major urgència, depenent de la seva gravetat.

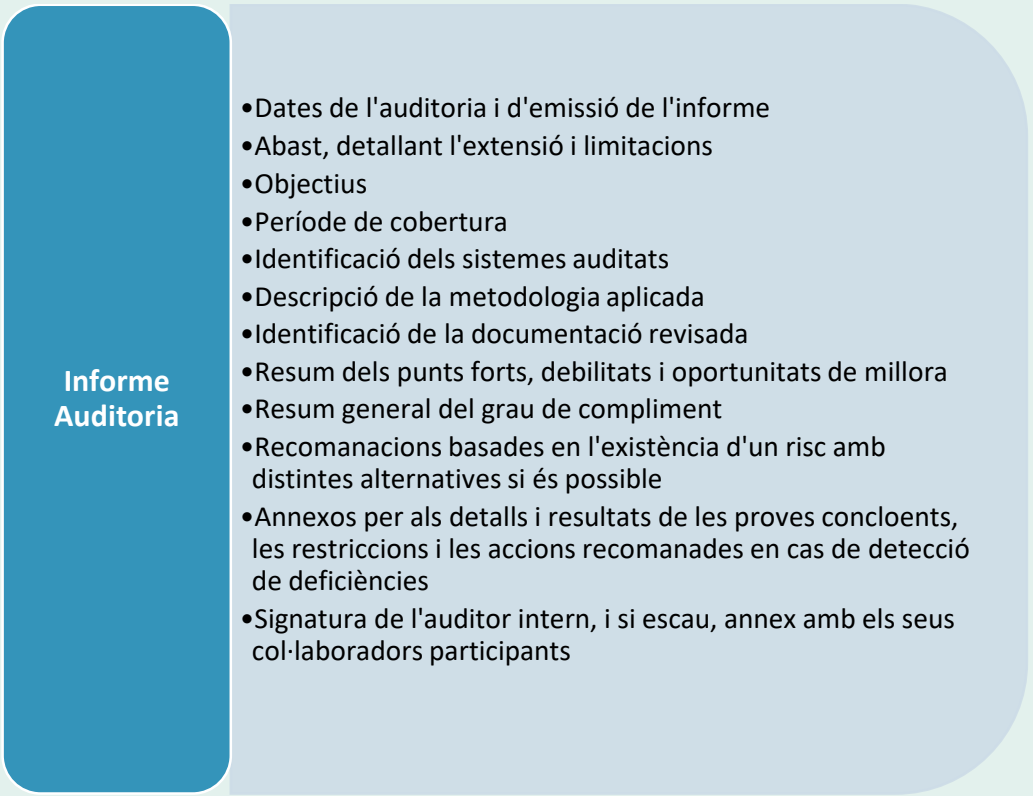


Figura 18. Contingut de l'informe final d'auditoria

Per altra banda, **tots els documents de treball que ha anat elaborant l'auditor intern** al llarg de l'auditoria haurien d'arxivar-se durant un període mínim de **dos anys**. La informació, que deuria guardar-se correctament referenciada i protegida, podria incloure els següents documents:

- Planificacions de les activitats incloses dins de l'auditoria interna
- Actes de les reunions amb els diversos participants i col·laboradors
- Captures de pantalla i d'altres proves efectuades
- Llistats

6.2. Seguiment de les accions correctives i preventives que cal executar

Tot el procés auditor haurà estat realment útil només si les mancances o vulnerabilitats detectades es resolen per complet o s'apliquen les mesures per preveure-les i reduir la probabilitat que es produeixin al màxim.

Per tant, en funció dels resultats obtinguts es proporcionaran una sèrie de **mesures correctores i/o preventives** a l'organització auditada, que hauran de quedar enregistrades i documentados.

A més, és convenient que s'estableixi el responsable encarregat d'implementar-les amb una programació del seu seguiment. Entre algunes de les mesures que l'auditor podria recomanar per a la seva incorporació posterior, depenent de les deficiències, es donarien les següents:

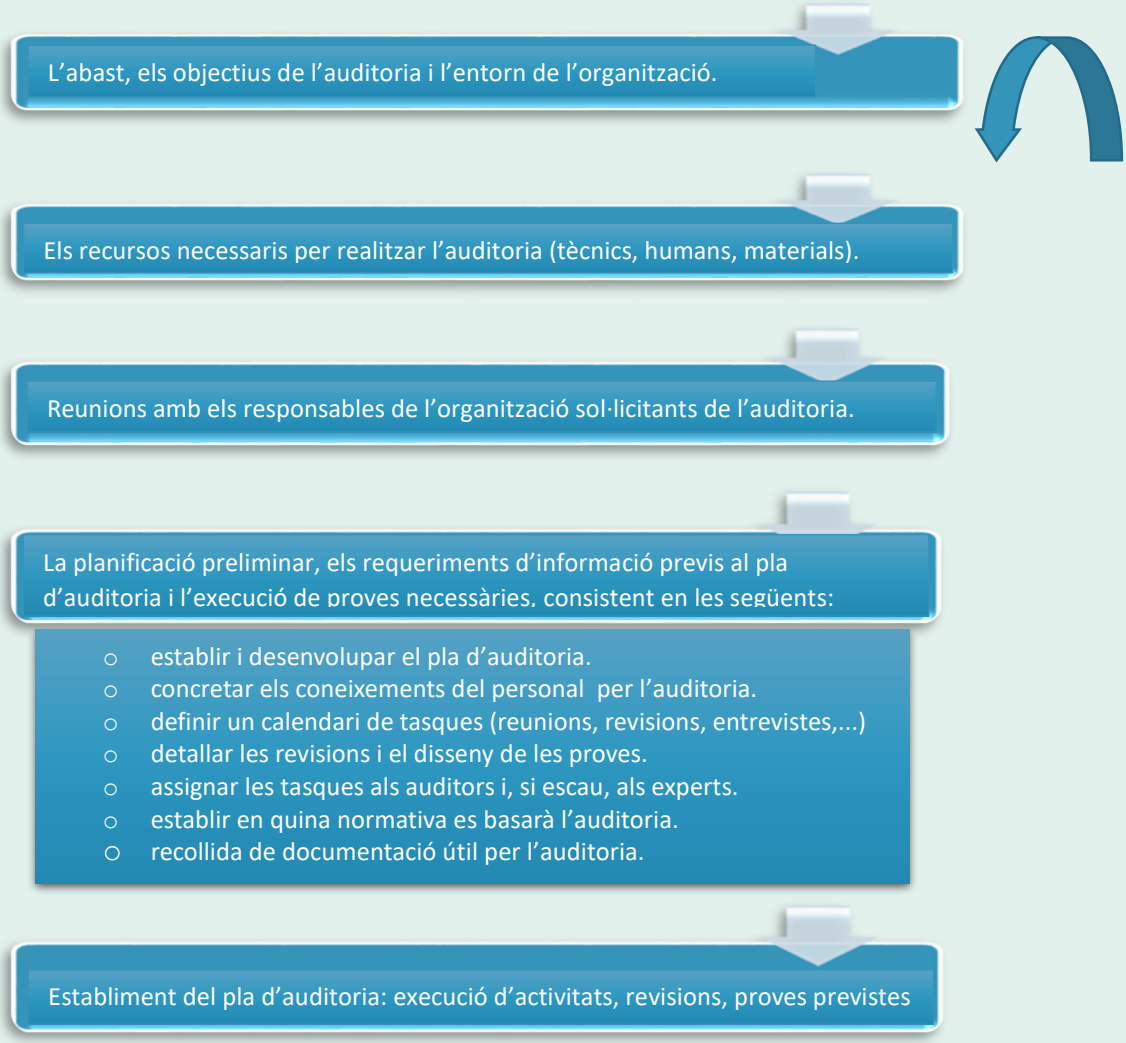
- Actualització dels antivirus per a que garanteixin convenientment una protecció eficaç.
- Reducció del risc d'atacs als actius per mitjà de l'externalització dels serveis amb la qual cosa s'evitarà la instal·lació de més equipament del necessari a l'organització.
- Elaboració de programes de formació dirigits als treballadors per millorar els seus coneixements, que alhora, beneficiarà a la seguretat dins de l'organització.
- Modificació de les polítiques de seguretat per introduir canvis en els procediments d'actualització de contrasenyes, d'accés més restringit,…
- Canvis a la infrastructura de xarxa, ja sigui de configuració o dels mateixos dispositius que la componen.
- Aplicació de pegats de seguretat i actualització del programari empresarial i dels sistemes operatius.
- Actualització de documents que contenen mancances o procediments desfasats.

Taula 19. Mesures correctores i preventives posteriors a l'auditoria interna

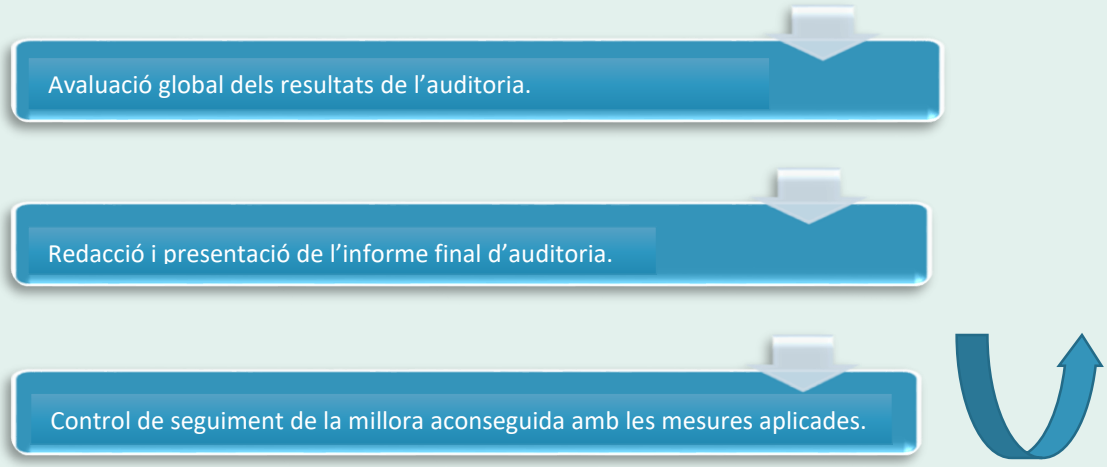
En el cas de les **accions correctives**, encaminades a resoldre els problemes que l'auditor ha observat, és convenient executar-les des del moment en què es té coneixement.

Quant a les **accions preventives**, que acostumen a ser suggerències de l'auditor sobre possibles millores en el sistema, ja que no responen a la detecció de problemes durant l'auditoria, la seva implantació es pot adoptar amb menor urgència però resulta molt aconsellable executar-les per obtenir millores en els sistemes.

En resum, tal com estableix la Guia de l'Auditoria de Seguretat de les TIC CCN-STIC 802[29] s'ha seguit la metodologia del desenvolupament i l'execució de l'auditoria en la que s'han anat succeïnt tots els pasos següents:



[29] Guía de Seguridad de las TIC CCN-STIC 802 ENS. Guía de auditoría [en línia]. [Consulta: 14 de novembre de 2022]. <https://www.ccn-cert.cni.es>



Taula 20. Metodologia del desenvolupament i execució de l'auditoria interna

Per a la implantació d'aquesta s'ha desenvolupat la metodologia PDCA *(Plan-Do-Check-Act)* en la qual es basa la norma ISO 27001:

- **Planificar**: es dissenyen les accions encaminades a estudiar en quina situació es troba la seguretat informàtica de l'organització, tenint en compte l'abast de l'auditoria, els objectius i els processos que s'hi desenvolupen.
- **Fer:** s'implementa el pla d'auditoria interna dissenyat i s'executen totes les accions i tasques conduents a la seva realització.
- **Comprovació:** es realitzen les comprovacions per avaluar i verificar a través del procés auditor que les mesures de seguretat implantades a l'organització són correctes i efectives. Si els resultats obtinguts indiquen l'existència de vulnerabilitats, s'elaboren les recomanacions conduents a la correcció o la reducció del risc.
- **Actuar:** S'executen les recomanacions o les mesures preventives i correctives que cal incorporar per millorar la seguretat dels sistemes d'informació. Però a més, es realitza un seguiment per comprovar que s'implanten les noves mesures i que realment aquestes resulten efectives.

Així, una vegada s'ha finalitzat cadascuna de les seves fases, fins arribar a la darrera, s'analitzen els resultats obtinguts, i després d'aplicar les millores escaients, es torna de nou a l'inici.

És a dir, amb el començament d'una nova auditoria, donat el seu **caràcter periòdic** i en què es segueix el **model PDCA en que tot el procés es torna a revisar**, s'assegura que es compleixin els objectius marcats per l'organització:

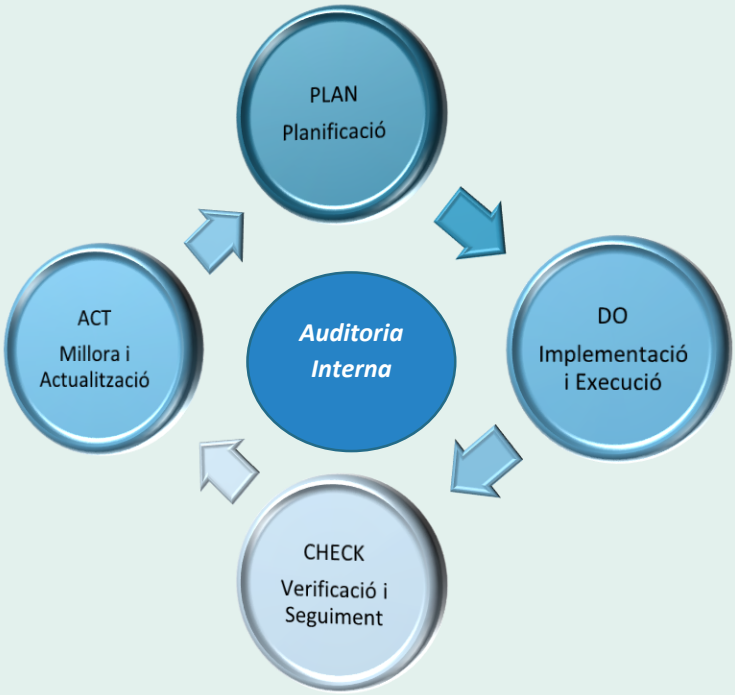


Figura 19. Model PDCA d'un procés auditor

7. Conclusions

Cada cop més, les organitzacions, amb l'auge de l'economia digital, disposen d'un major nombre d'eines tecnològiques, que utilitzades i protegides de forma convenient, permeten que aquestes siguin molt més productives, però en cas contrari, també és cert que poden produir-les greus perjudicis. Sobretot pel que fa a **la informació, com a principal recurs valuós que s'ha de considerar** com a part integral de tot el cicle de vida dels sistemes d'informació.

És per això, que anualment, les organitzacions haurien de planificar auditories internes per determinar si els seus processos d'informació i sistemes informàtics compleixen amb els **requeriments estàndards i la normativa vigent** aplicables a la seguretat informàtica.

De fet, **moltes organitzacions desconeixen les vulnerabilitats i les amenaces** a les quals es troben exposats els seus sistemes, i és gràcies a aquestes auditories com podrien prendre-hi consciència per començar a emprendre les accions oportunes per reduir el risc.

L'auditoria interna deuria considerar la importància de les **diferents àrees de l'organització, els seus processos i l'efectivitat de les mesures aplicades a auditories anteriors** en cas que ja

haguessin tingut lloc. A més, s'ha de considerar com un procés que cal realitzar periòdicament degut a **l'entorn canviant** existent que origina una contínua transformació dels riscos, i per tant, la necessitat d'actualitzar tots aquells procediments i mecanismes encaminats a la protecció dels sistemes informàtics.

Per al seu correcte desenvolupament, l'auditor ha d'executar **aquest procés de forma documentada i amb total objectivitat** des del moment en que comença a planificar-lo fins que el finalitza amb l'informe final.

A més, a més, per a que l'auditoria sigui exitosa i efectiva, és imprescindible **la participació de tota l'organització**, i especialment, **el compromís per part de la Direcció,** que ha de ser conscient de la importància de desenvolupar aquest procés degut als avantatges que reporta per a l'activitat empresarial.

Per altra banda, cal considerar la importància del factor humà en la seguretat informàtica. En relació a això, l'auditoria interna contribueix a aportar **una major eficiència i rendibilitat dels recursos humans** perquè, d'una banda, a partir de l'aplicació de les proves, la retroalimentació i les evidències obtingudes, es podran dissenyar accions formatives més adients a les necessitats de seguretat informàtica de l'organització, que crearan una major cultura de seguretat entre els seus usuaris, i d'altra, facilitarà les seves tasques amb l'elaboració de millores als aplicatius que fan servir a diari.

Així mateix, és fonamental **l'aplicació de les recomanacions i mesures correctores obtingudes a la finalització del procés auditor** a fi de prevenir o resoldre les deficiències detectades, ja sigui mitjançant la modificació o la inclusió de nous procediments de treball, l'execució de determinades accions o la realització de canvis en els aplicatius o el maquinari a fi d'evitar que es materialitzin situacions potencials de risc.

Tot això, sense oblidar de realitzar posteriorment una **activitat de seguiment per avaluar que s'assoleixen els objectius marcats** a fi d'evitar impactes perniciosos a la seguretat informàtica al permetre una resposta eficaç davant successos externs o interns que la podrien afectar.

Per tant, durant l'elaboració del treball **s'ha après la importància que prenen, no només les qüestions més directament relacionades amb la seguretat informàtica**, sinó també d'altres com les legals, que moltes vegades podrien passar desapercebudes per desconeixement, però que s'han d'incloure necessàriament. Per això, és important comptar amb col·laboradors de diverses matèries, que poden assessorar en altres aspectes que també afecten al desenvolupament òptim de l'auditoria.

A mode de reflexió, cal afegir que en aquest projecte s'ha analitzat com crear un model a seguir pel mateix auditor intern per facilitar-li el desenvolupament d'una auditoria interna de seguretat informàtica, que tal com s'ha esmentat anteriorment, es podria aplicar a qualsevol organització. Per tant, funcionaria com **una guia a fi que l'auditor pogués planificar la seva auditoria**, aconseguint un resultat eficient, sigui quin sigui l'àmbit de l'activitat de negoci per contribuir a la millora de la seguretat informàtica.

Sobretot, perquè **dins de l'àmbit de les auditories internes és força escassa la bibliografia existent**, mentre que està molt més desenvolupada la que fa referència a les auditories externes. Com a conseqüència, sempre han estat més conegudes les auditories externes que realitzen les empreses per poder obtenir la certificació. En canvi, tot i que l'auditoria interna no suposa l'obtenció directa de la certificació, sí que pot ser un procés facilitador de la seva obtenció, i a més, executada de forma periòdica, contribueix a garantir innombrables avantatges (...) de forma permanent, però **està molt desaprofitada ja que actualment no es troba prou estesa**, i podria aportar molt valor afegit a les organitzacions on s'introduís.

Per tal de realitzar un seguiment del treball, es va crear **un calendari consistent en desglossar el conjunt de tasques** necessàries per detallar la planificació de l'auditoria interna, distribuïnt-les en un o diversos dies, depenent del seu grau de complexitat o del temps calculat per tal d'assolir una determinada tasca.

Com que aquesta calendarització, que es mostra als annexos I i II, ja pressuposa que pot haver en algun moment algun tipus d'imprevist, s'ha intentat no ajustar-la de forma massa estricta, de forma que s'ha pogut desenvolupar tot el procés que implica dins de les dates previstes fins arribar a la seva finalització.

Com a línia de treball futur seria molt interessant que tot el que s'ha exposat de forma teòrica al llarg d'aquest model d'auditoria interna, **es posés en pràctica en organitzacions de característiques diferents** (tamany, sector, tipologia de processos que desenvolupen,...) per comprovar que s'assoleixen tots els objectius que persegueix l'auditoria, i que tal com es preveu, els resultats obtinguts són d'una rellevància significant. A més, seria interessant comprovar posteriorment, que aquesta mateixa aplicació de l'auditoria interna en una situació real, **resulta apta per obtenir la certificació** que atorga una auditoria externa.

A més, una altra qüestió a tenir en compte pel que fa a la planificació d'auditories internes futures, és que previsiblement pot necessitar de canvis per actualitzar-la o per ampliar el seu camp d'acció per tal de no quedar obsoleta, donada la contínua evolució dins d'un àmbit que exigeix una constant posada al dia, com és el de la seguretat informàtica. És per aquesta raó, que **l'auditoria interna que s'exposa en aquest treball s'ha de considerar com un procés** no estàtic, sinó **necessàriament dinàmic.**

En resum, cap organització deuria d'ajornar una auditoria interna perquè aquesta suposarà un **procés de millora contínua**, que contribuirà a un funcionament correcte dels seus equips i sistemes d'informació. Tot això, amb l'avantatge afegit de poder disposar de mesures preventives i/o correctores que ajudaran a reduir de forma molt significativa els riscos i respondre amb major antelació davant de qualsevol incident, garantint la continuïtat de l'activitat empresarial.

8. Glossari

Actius informàtics: Són els recursos, tant físics com lògics d'un sistema d'informació o en relació amb aquest, que es fan necessaris per a que una organització pugui desenvolupar les seves activitats.

Atacs informàtics: Són aquells successos intencionats, que tenint éxit o no, intenten afectar el bon funcionament del sistema informàtic.

Amenaça: causa potencial d'un incident indesitjat que pot danyar un sistema.

Auditor: Persona amb les capacitats i coneixements necessaris per poder realitzar una auditoria.

Auditoria: Revisió sistemàtica que es realitza per avaluar si es compleixen unes regles o directrius destinades a garantir el bon funcionament d'una activitat.

BYOD (*Bring Your Own Device*): Fa referència a l'ús laboral de dispositius i aplicacions que són propietat del propi empleat.

Certificació: És una acta mitjançant la qual es pot demostrar que es compleixen certs requisits.

Ciberseguretat: Amb la irrupció del ciberespai, sorgeix aquesta disciplina en relació a la seguretat informàtica, orientada cap a la defensa i anticipació de les amenaces que poden afectar a la informació i als sistemes que treballen sota aquest entorn.

Commutador (switch): Dispositiu de la xarxa que permet comunicar els dispositius que la integren entre sí per compartir recursos.

Confidencialitat: Propietat de la informació que garanteix que aquesta sigui accessible només al personal autoritzat.

Control d'accés: Mecanisme per proporcionar un accés autoritzat només a aquell que es pot autenticar correctament.

Criticitat: Aspecte d'un recurs que indica la importància que suposa per poder mantenir l'activitat empresarial funcionant de forma acceptable.

Defectes: S'aplica als requeriments d'un element quan aquest no funciona segons s'esperava o s'havia contractat (per ex. un programari que produeix errors per un mal disseny).

Desastre: Interrupció en els sistemes informàtics d'una organització que desemboca en la incapacitat per poder accedir o processar informació, cosa que impedeix la seva normal activitat.

Delicte informàtic: Aquell delicte que té lloc per mitjà de l'ús de la tecnologia informàtica.

Disponibilitat: És la propietat que indica que el sistema pot recuperar-se ràpidament davant de qualsevol contingència, tot i que també es pot aplicar als recursos en referència a que aquests poden ser utilitzats pels usuaris en qualsevol moment.

Doble factor d'autenticació: Mètode d'autenticació electrònica en el qual es proporciona l'accés si es superen dos o més factors a un mecanisme d' autenticació, consistents en alguna cosa que l'usuari coneix, té o posseeix.

DRP: Pla de recuperació de desastres que té la finalitat de garantir l'activitat de l'organització després d'un desastre a través de la restauració de les seves dades, el maquinari i el programari més crítics.

Eficiència: Capacitat que indica que el rendiment és adequat, en relació al consum de recursos i temps i sota unes condicions ja establertes.

Encaminador (router): Dispositiu de xarxa encarregat de l'enviament de paquets de dades entre xarxes de computadors.

Enginyeria social: Tècniques de persuasió utilitzades per obtenir informació de manera no autoritzada, amb la intenció d'obtenir un benefici econòmic o per realitzar altres atacs.

Estándar ANSI/EIA/TIA-568: és un estàndard per a l'instal·lació de cablejat d'edificis comercials que estableix els elements i medis de connexió de les xarxes de telecomunicacions.

Estratègia: Conjunt d'accions que es duen a terme, fixant prèviament els recursos necessaris per desenvolupar-les, amb la finalitat d'assolir un resultat determinat.

Evidència: Registre o informació basada en fets comprovables.

IDS: Sistemes de Detecció d'Intrusions que permet detectar els accessos no autoritzats a un sistema informàtic.

Impacte: Són les conseqüències que se'n poden derivar en cas que es materialitzi un risc.

Incident: Succés que es produeix com a conseqüència d'haver superat les mesures de seguretat: destrucció d'informació, suplantació d'identitat, robatori d'equips informàtics,...

Integritat: Qualitat de la informació segons la qual aquesta es manté inalterada, davant d'incidents d'accés no autoritzats interns o externs de caràcter maliciós que poden modificar-la o eliminar-la.

ISO: Organització Internacional per a l'Estandardització.

IEC: Comissió Electrotècnica Internacional.

ISO/IEC 27001:2017: Norma estàndard que recull els requeriments necessaris per garantir una gestió adequada de la informació, assegurant la seva confidencialitat, integritat i disponibilitat.

ISO/IEC 27002:2022: Norma estàndard per a la seguretat de la informació publicat per l'Organització Internacional de Normalització i la Comissió Electrotècnica Internacional.

Magerit: Metodologia d'anàlisi de riscos, el resultat de la qual permet recomanar les mesures que permetin reduir els danys o perjudicis que podrien originar aquests riscos.

Manteniment correctiu: És aquell destinat a resoldre les avaries o fallades existents.

Manteniment preventiu: És aquell conjunt de mesures que es duen a terme per evitar o reduir el risc que es pugui presentar una fallada al maquinari o al programari.

Norma UNE-EN 50173: Estàndard del cablejat estructurat que estableix les directrius de diversos serveis de comunicació a les organitzacions.

Phising o robatori d'identitat: Delicte informàtic consistent en el frau que es comet fent ús de l'enginyeria social per aconseguir informació confidencial.

Pla de contingència: Conjunt de procediments que proporciona una solució alternativa per tal de garantir la continuïtat de l'activitat davant algun incident que afecti en part o totalment als sistemes d'informació d'una organització.

Procés de millora contínua: Procés que serveix per a millorar de forma constant les empreses sense necessitat de realitzar grans canvis.

Ransomware: és un programari maliciós que pot arribar a xifrar la informació dels equips informàtics, de forma que els atacants reclamen posteriorment un pagament per rescatar aquesta informació, tot i que fins i tot, en el cas d'efectuar el seu pagament no hi ha garanties de recuperar-la.

Resultats de l'auditoria: Són els obtinguts una vegada finalitzada l'avaluació realitzada durant l'auditoria atenent als criteris acordats inicialment. Aquests permeten elaborar l'informe final amb les mesures correctores escaients.

Risc: És la possibilitat que es produeixi un impacte sobre algun element de l'organització, que pot venir donat per un fenomen natural o artificial. Depenent de l'element que hagi estat afectat, pot tenir un abast més o menys ampli o greu (pèrdues humanes, interrupció de l'activitat econòmica, danys materials,...)

Salvaguarda: Mesures o procediments tecnològics encaminats a la reducció del risc. Poden actuar amb la limitació del dany que es podria produir com a conseqüència de les amenaces, o bé, reduir la freqüència amb la que aquestes es poden presentar.

Seguretat informàtica: Conjunt de mesures dirigides cap a la preservació dels actius d'informació per tal d'evitar la seva modificació, eliminació o divulgació de forma intencionada o accidental, per a que l'activitat pugui desenvolupar-se amb normalitat a diari.

SIEM: Sistema que emmagatzema informació de la xarxa durant períodes prolongats de temps per analizar-la i detectar en temps real amenaces que neutralitza ràpidament per evitar atacs a l'infrastructura tecnològica d'una organització.

Tallafocs (firewalls): Maquinari o programari que filtra i examina els fluxos d'informació que arriben a través de la connexió a Internet, de forma que pot evitar un atac a la xarxa o a la seva informació.

Teletreball: És el treball a distància que pot realitzar-se aprofitant l'existència de noves tecnologies com Internet.

TIC: Tecnologies de la Informació i la Comunicació.

VLAN: Mecanisme segons el qual es creen xarxes lògiques independents dins d'una mateixa xarxa física.

VPN: Xarxa privada virtual que permet treballar a un empleat fora del seu lloc de treball a l'autenticar la connexió des de l'exterior per mitjà de les seves credencials. A més, la informació amb la que treballa es transmet xifrada, pel que és una xarxa molt utilitzada pels teletreballadors.

Vulnerabilitats: Són aquelles deficiències, l'existència de les quals pot ser aprofitada per les amenaces per produir un dany sobre els actius d'informació.

Zona desmilitaritzada (DMZ): Subxarxa entre la xarxa Internet i la xarxa privada a la que protegeix.

9. Bibliografia

- ✓ ISO27000 [en línia]. [Consulta: 30 de setembre de 2022]. <http://www.iso.org>
- ✓ Los principales cambios de la actualización de la norma ISO 27002:2022 [en línia]. [Consulta: 2 d'octubre de 2022]. <https://www.globalsuitesolutions.com/es/cambios-norma-iso-27002-2022>
- ✓ Fenz, S. and Neubauer, T. (2018), "Ontology-based information security compliance determination and control selection on the example of ISO 27002", Information and Computer Security, Vol. 26 No. 5, pp. 551-567 [en línia]. [Consulta: 1 d'octubre de 2022]. <https://doi.org/10.1108/ICS-02-2018-0020>
- ✓ Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS [en línia]. [Consulta: 1 d'octubre de 2022]. <http://joiv.org/index.php/joiv/article/download/482/298>
- ✓ Patiño, S., Caicedo, A., & Guaña, E. R. (2019). Modelo de evaluación del dominio control de acceso de la norma ISO 27002 aplicado al proceso de gestión de bases de datos. Revista Ibérica De Sistemas e Tecnologias De Informação, 230-241 [en línia]. [Consulta: 1 d'octubre de 2022]. <https://www.proquest.com/scholarly-journals/modelo-de-evaluación-del-dominio-control-acceso/docview/2317841707/se-2

- ✓ Nueva ISO/IEC 27002:2022: cambios con respecto a la versión de 2013 [en línia]. [Consulta: 2 d'octubre de 2022]. <https://www.isotools.org/2022/07/22/nueva-iso-iec-270022022-cambios-con-respecto-a-la-version-de-2013/#:~:text=La%20respuesta%20a%20incidentes%20de%20seguridad%20de%20ISO%2FIEC,informaci%C3%B3n.%20Algunos%20de%20los%20cambios%20m%C3%A1s%20relevantes%20son%3A>

- ✓ ISO 27002: Buenas prácticas para gestión de la seguridad de la información [en línia]. [Consulta: 2 d'octubre de 2022]. <https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi>

- ✓ Evaluación de sistemas de seguridad informáticos universitarios Caso de Estudio: Sistema de Evaluación Docente [en línia]. [Consulta: 2 d'octubre de 2022]. <https://www.proquest.com/scholarly-journals/evaluación-de-sistemas-seguridad-informáticos/docview/2317841275/se-2>

- ✓ Llei 59/2003, de 19 de desembre, de signatura electrònica [en línia]. [Consulta: 22 d'octubre de 2022]. <https://portaljuridic.gencat.cat/ca/document-del-pjur/?documentId=668429>

- ✓ Constitució espanyola [en línia]. [Consulta: 22 d'octubre de 2022]. <https://www.senado.es/web/conocersenado/normas/constitucion/index.html?lang=ca_ES>

- ✓ Carta dels drets fonamentals de la Unió Europea [en línia]. [Consulta: 22 d'octubre de 2022]. <https://barcelona.spain.representation.ec.europa.eu/publications/carta-dels-drets-fonamentals-de-la-unio-europea_ca>

- ✓ Tratado de funcionamiento de la Unión Europea [en línia]. [Consulta: 22 d'octubre de 2022]. <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:C:2016:202:TOC>

- ✓ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [en línia]. [Consulta: 23 d'octubre de 2022]. <https://www.boe.es/eli/es/lo/2018/12/05/3/con>

- ✓ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico [en línia]. [Consulta: 23 d'octubre de 2022]. <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

- ✓ Ley 11/2022, de 28 de junio, General de Telecomunicaciones [en línia]. [Consulta: 22 d'octubre de 2022]. <https://www.boe.es/buscar/act.php?id=BOE-A-2022-10757>

- ✓ Ley 17/2001, de 7 de diciembre, de Marcas [en línia]. [Consulta: 23 d'octubre de 2022]. <https://boe.es/buscar/act.php?id=BOE-A-2001-23093>

- ✓ Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques [en línia]. [Consulta: 23 d'octubre de 2022].

<http://www.caib.es/sites/transparenciaperconselleria/ca/n/ley_392015_de_1_de_octubre_del_procedimiento_administrativo_coman_de_las_administraciones_pablicas>

- ✓ Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia [en línia]. [Consulta: 23 d'octubre de 2022]. <https://boe.es/buscar/act.php?id=BOE-A-1996-8930>

- ✓ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [en línia]. [Consulta: 20 d'octubre de 2022]. <https://boe.es/buscar/act.php?id=BOE-A-1999-23750>

- ✓ Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica ("BOE" 274, de 15 - 11 - 2002) [en línia]. [Consulta: 22 d'octubre de 2022]. <http://www.boe.es/boe_catalan/dias/2002/12/02/pdfs/A03057-03062.pdf>

- ✓ LLEI 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica [en línia]. [Consulta: 21 d'octubre de 2022]. <https://dogc.gencat.cat/ca/document-del-dogc/?documentId=246194>

- ✓ Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal [en línia]. [Consulta: 24 d'octubre de 2022]. <https://www.boe.es/eli/es/lo/1995/11/23/10/con>

- ✓ Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure [en línia]. [Consulta: 24 d'octubre de 2022]. <https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf>

- ✓ El estado de la ciberseguridad en España | Deloitte España [en línia]. [Consulta: 30 de setembre de 2022]. <https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html>

- ✓ Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria [en línia]. [Consulta: 1 d'octubre de 2022]. <https://dialnet.unirioja.es/servlet/articulo?codigo=4670355#:~:text=Gu%C3%ADa%20de%20buenas%20pr%C3%A1cticas%20de%20seguridad%20inform%C3%A1tica%20en,Idioma%3A%20espa%C3%B1ol%204%20T%C3%ADtulos%20paralelos%3A%20...%20M%C3%A1s%20elementos>

- ✓ Auditoría interna y los riesgos de la ciberseguridad. [10 d'octubre de 2022]. [Consulta:]. <https://www.bing.com/ck/a?!&&p=26ae1e58b7ca88d4JmltdHM9MTY2NzYwNjQwMCZpZ3VpZD0zMjdlMDNiNy0xMDJjLTZlNmEtMGU2NC0xMWU0MTE2NTZmZWUmaW5zaWQ9NTE3OQ&ptn=3&hsh=3&fclid=327e03b7-102c-6e6a-0e64-11e411656fee&psq=Auditor%c3%ada+interna+y+los+riesgos+de+la+ciberseguridad.+KPMG

&u=a1aHR0cHM6Ly9hc3NldHMua3BtZy9jb250ZW50L2RhbS9rcG1nL2FyL3BkZi8yMDIwL2F1ZGl0b3JpYS1pbnRlcm5hLXktbG9zLXJpZXNnb3MtZGUtY2liZXJzZWd1cmlkYWQucGRm&ntb=1>

- ✓ Magerit-versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información [en línia]. [Consulta: 2 d'octubre de 2022]. <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html>

- ✓ Guía de buenas prácticas para auditar la ciberseguridad [en línia]. [Consulta: 2 d'octubre de 2022]. <https://www.asobancaria.com/wp-content/uploads/2022/06/Guia_de_Buenas_Practicas_para_Auditar_la_Ciberseguridad_2022_V1.pdf>

- ✓ Manual de seguridad informática en la empresa-Proyecto Competic [en línia]. [Consulta: 1 d'octubre de 2022].<https://economia.jcyl.es/web/jcyl/binarios/596/823/Manual%20Ciberseguridad%20ESPA%C3%91OL.pdf?blobheader=application%2Fpdf%3Bcharset%3DUTF-8&blobnocache=true>

- ✓ Implantación de un SGSI en la empresa [en línia]. [Consulta: 14 d'octubre de 2022]. <https://www.lawebdelprogramador.com/pdf/5798-Implantacion-de-un-SGSI-en-la-empresa.html>

- ✓ Protección de la información [en línia]. [Consulta: 15 d'octubre de 2022]. <https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf>

- ✓ Elaboración de un plan para la implementación del sistema de gestión de seguridad de la información [en línia]. [Consulta: 15 d'octubre de 2022]. <https://openaccess.uoc.edu/handle/10609/19067>

- ✓ Guía de iniciación a actividad profesional. Implantación de sistemas de gestión de la seguridad (SGSI) según la norma ISO 27001 [en línia]. [Consulta: 17 d'octubre de 2022]. <https://www.coit.es/informes/implantacion-de-sistemas-de-gestion-de-la-seguridad-de-la-informacion-sgsi-segun-la-norma>

- ✓ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) [en línia]. [Consulta: 20 d'octubre de 2022]. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>

- ✓ Reglament (UE) 2022/868 del Parlament Europeu i del Consell, de 30 de maig de 2022, relatiu a la governança europea de dades i pel qual es modifica el Reglament (UE) 2018/1724 (Reglament de governança de dades) [en línia]. [Consulta: 21 d'octubre de 2022].

https://apdcat.gencat.cat/web/.content/01-autoritat/normativa/documentos/Data-governance-act.pdf

- ✓ Decálogo ciberseguridad empresas: una guía de aproximación para el empresario [en línia]. [Consulta: 25 d'octubre de 2022]. <https://www.incibe.es/protege-tu-empresa/blog/decalogo-ciberseguridad-empresas-guia-aproximacion-el-empresario>

- ✓ Arquitectura de red segura, las cosas en orden [en línia]. [Consulta: 15 d'octubre de 2022]. <https://www.incibe-cert.es/blog/arquitectura-red-segura-las-cosas-orden>

- ✓ Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals [en línia]. [Consulta: 20 d'octubre de 2022]. <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673>

- ✓ El IEC 62443-4-2, la necesidad de securizar los componentes [en línia]. [Consulta: 22 d'octubre de 2022]. <https://www.incibe-cert.es/blog/el-iec-62443-4-2-necesidad-securizar-los-componentes>

- ✓ Top 10 vulnerabilidades web de 2021 [en línia]. [Consulta: 9 d'octubre de 2022]. <https://www.incibe.es/protege-tu-empresa/blog/top-10-vulnerabilidades-web-2021>

- ✓ Castillo, A., Hidalgo, J. & Guano, C. (Julio - diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

- ✓ *Análisis de una red en un entorno IPV6: una mirada desde las intrusiones de red y el modelo tcp/ip*. Universidad Francisco de Paula Santander Ocaña. Colombia: Revista Colombiana de Tecnologías de Avanzada, 2017-, vol. 1, núm. 29. ISSN: 1692-7257

- ✓ Análisis y captura de paquetes de datos en una red mediante la herramienta Wireshark [en línia]. [Consulta: 24 de novembre de 2022]. <http://repositorio.uisrael.edu.ec/bitstream/47000/168/1/UISRAEL-EC-SIS-378.242-404.pdf>

- ✓ Standards ANSI/TIA/EIA 568-B Commercial Building Telecommunications Cabling Standard [en línia]. [Consulta: 29 de novembre de 2022]. <https://www.bing.com/ck/a?!&&p=9733e060c3be32f4JmltdHM9MTY2OTc2NjQwMCZpZ3VpZD0zNjZmMWU3Ni1mNzM1LTZjMjUtMzYwYi0wYzFhZjY3YzZkMDYmaW5zaWQ9NTE5OA&ptn=3&hsh=3&fclid=366f1e76-f735-6c25-360b-0c1af67c6d06&psq=ANSI%2fEIA%2fTIA-568&u=a1aHR0cHM6Ly93d3cuY3NkLnVvYy5nci9-aHk0MzUvbWF0ZXJpYWwvQ2FibGluZyUyMFN0YW5kYXJkJTIwLSUyMEFOU0ktVElBLUVJQSUyMDU2OCUyMEIlMjAtJTIwQ29tbWVyY2lhbCUyMEJ1aWxkaW5nJTIwVGVsZWNvbW11bmljYXRpb25zJTIwQ2FibGluZyUyMFN0YW5kYXJkLnBkZg&ntb=F>

Imatges de la pàgina 7:

- ✓ https://cdn.pixabay.com/photo/2014/08/14/10/38/software-417880__480.jpg
- ✓ https://pixabay.com/es/vectors/computadora-escritorio-303726
- ✓ https://pixabay.com/es/illustrations/red-computadora-computadora-port%c3%a1til-698598
- ✓ https://pixabay.com/es/illustrations/seguro-castillo-1435364

- ✓ Guía de Seguridad de las TIC CCN-STIC 802 ENS. Guía de auditoría [en línia]. [Consulta: 14 de novembre de 2022]. <https://www.ccn-cert.cni.es>

- ✓ Protege tu información, aplica estas recomendaciones de seguridad en servicios de almacenamiento cloud | INCIBE [en línia]. [Consulta: 14 de novembre de 2022]. https://www.incibe.es/protege-tu-empresa/blog/protege-tu-informacion-aplica-estas-recomendaciones-seguridad-servicios

- ✓ Protección de la información. [en línia]. [Consulta: 14 de novembre de 2022]. <https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion>

- ✓ Buenas prácticas en el área de informática | INCIBE [en línia]. [Consulta: 1 d'octubre de 2022]. https://www.incibe.es/protege-tu-empresa/que-te-interesa/buenas-practicas-area-informatica

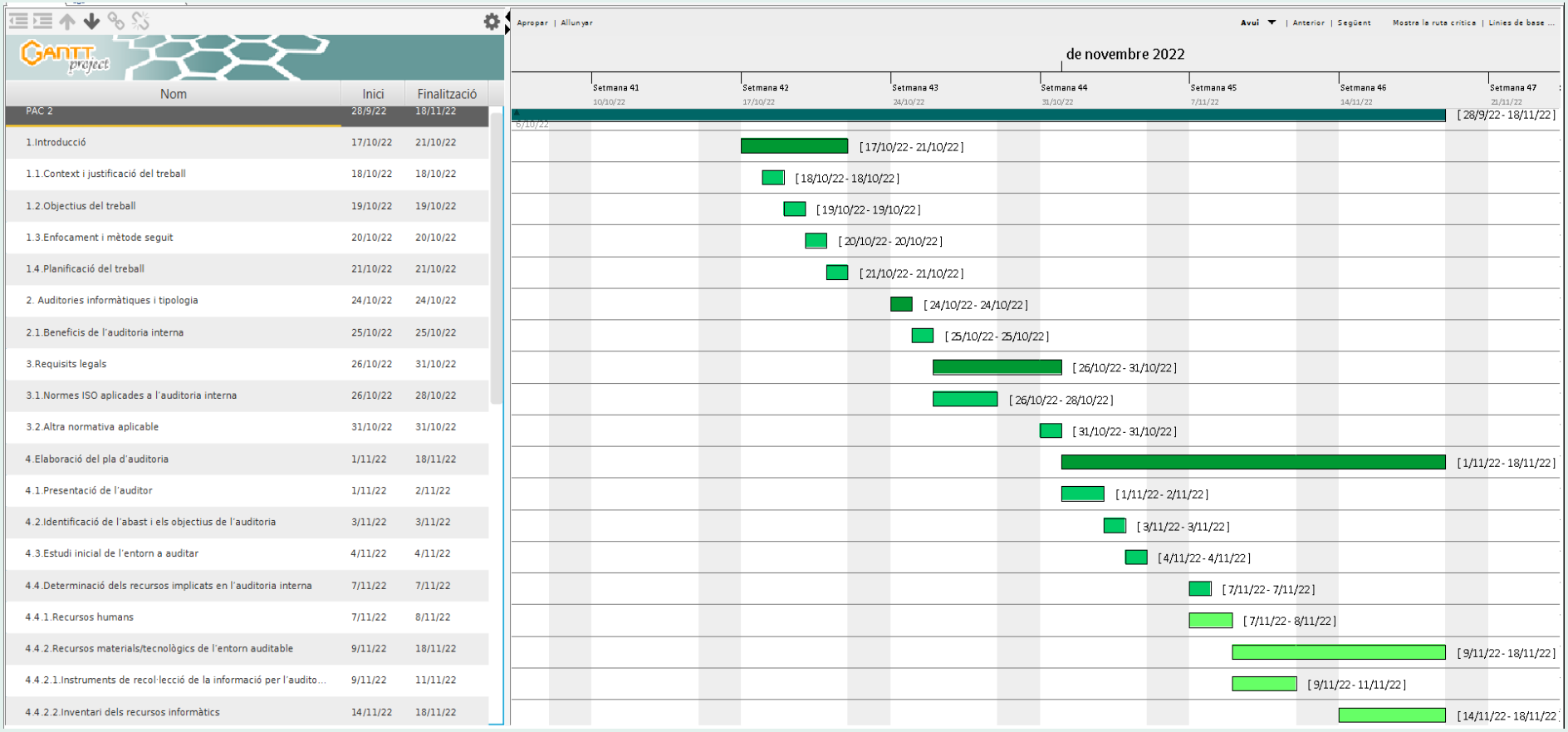
- ✓ Decálogo ciberseguridad empresas. Una guía de aproximación para el empresario [en línia]. [Consulta: 3 de desembre de 2022]. https://www.incibe.es/protege-tu-empresa/guias/decalogo-ciberseguridad-empresas-guia-aproximacion-el-empresario

- ✓ Automatizando inyecciones con SQLMAP [en línia]. [Consulta: 16 de desembre de 2022]. https://blog.isecauditors.com/2019/12/automatizando-inyecciones-con-sqlmap.html?m=1

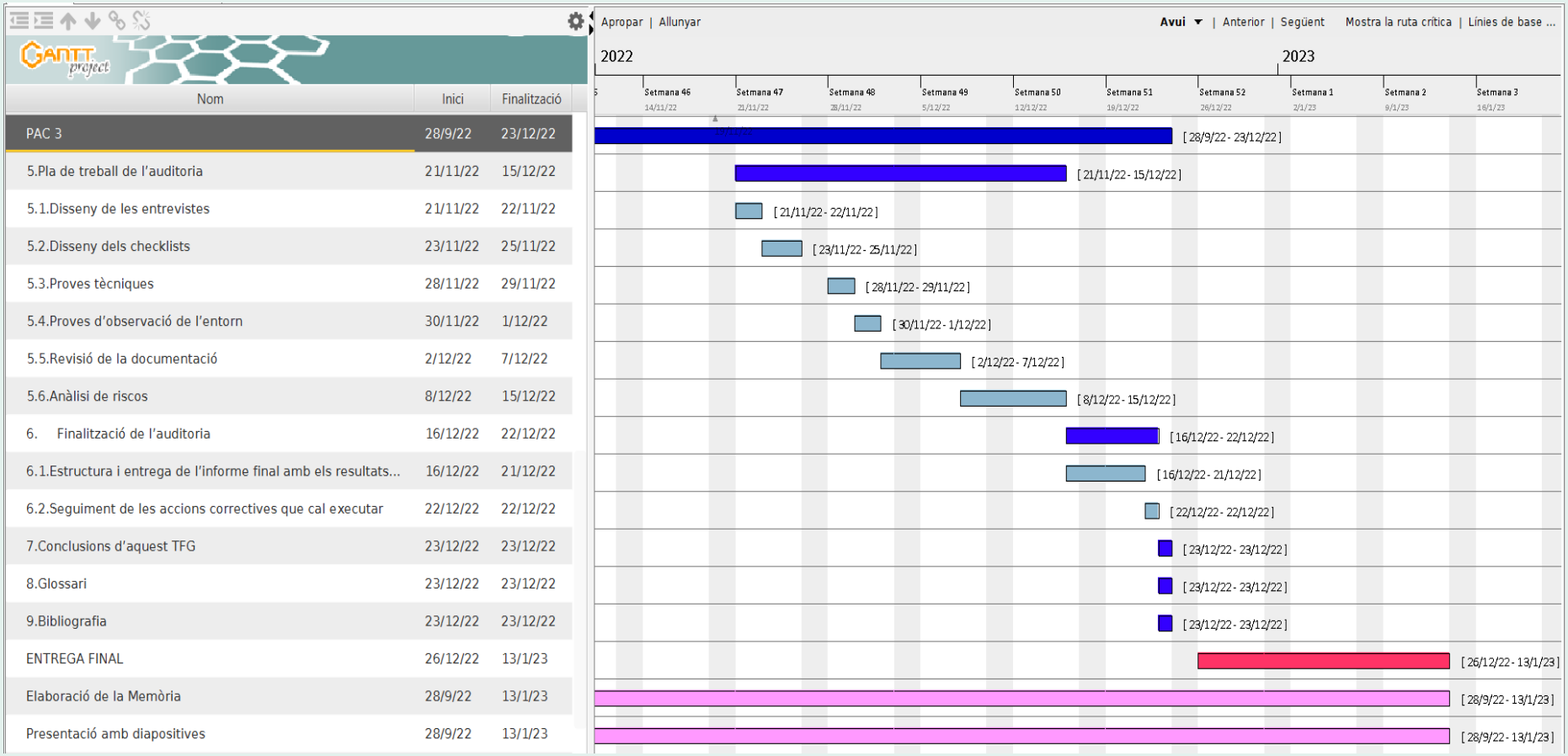
- ✓ Robayo, L. A. (2021). Vulnerabilidades informáticas en implementaciones con el cms wordpress. [Monografia]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/40343

- ✓ *Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web.* Universitat de Guadalajara. Mèxic: ReCIBE, 2015, núm. 1. ISSN: 2007-5448 [en línia]. [Consulta: 16 de desembre de 2022]. https://www.redalyc.org/pdf/5122/512251501005.pdf

Annex I. Planificació del treball de l'auditoria interna (PAC 2)



Annex II. Planificació del treball de l'auditoria interna (PAC 3)



Nom	Inici	Finalització
PAC 3	28/9/22	23/12/22
5.Pla de treball de l'auditoria	21/11/22	15/12/22
5.1.Disseny de les entrevistes	21/11/22	22/11/22
5.2.Disseny dels checklists	23/11/22	25/11/22
5.3.Proves tècniques	28/11/22	29/11/22
5.4.Proves d'observació de l'entorn	30/11/22	1/12/22
5.5.Revisió de la documentació	2/12/22	7/12/22
5.6.Anàlisi de riscos	8/12/22	15/12/22
6. Finalització de l'auditoria	16/12/22	22/12/22
6.1.Estructura i entrega de l'informe final amb els resultats...	16/12/22	21/12/22
6.2.Seguiment de les accions correctives que cal executar	22/12/22	22/12/22
7.Conclusions d'aquest TFG	23/12/22	23/12/22
8.Glossari	23/12/22	23/12/22
9.Bibliografia	23/12/22	23/12/22
ENTREGA FINAL	26/12/22	13/1/23
Elaboració de la Memòria	28/9/22	13/1/23
Presentació amb diapositives	28/9/22	13/1/23