ISO, gestió integral. Guia pràctica per a la correcta aplicació de la normativa vigent en les organitzacions empresarials.

Gerard Vila Truco

Grau en Enginyeria de Tecnologies i Serveis de Telecomunicació

Àrea: Administració de xarxes y Sistemes Operatius

Tutora: Arianna Arlet Garrido Blanes

Juny 2023

Agraïments

Voldria mostrar el meu agraïment als meus amics i a la meva família.

Especialment, als meus pares, Josep Maria i Dèlia, i al meu germà, Albert per la seva paciència, suport i ajuda al llarg d'aquest temps, sense ells no ho hauria aconseguit.

A la meva tutora del TFG, Arianna Arlet Garrido Blanes, pel seu rigor, el seu interès, la seva disposició i constant col·laboració en la realització d'aquest treball.

“ *Vincit qui patitur*

Gerard Vila Truco

FITXA DEL TREBALL FINAL

Títol del treball:	*ISO, gestió integral. Guia pràctica per a la correcta aplicació de la normativa vigent en les organitzacions empresarials.*
Nom del autor:	*Gerard Vila Truco*
Nom de la consultora:	*Arianna Arlet Garrido Blanes*
Nom del PRA:	*David Bañeres Besora*
Data d'entrega (mm/aaaa):	*06/2023*
Titulació:	*Grau en Enginyeria de Tecnologies i Serveis de Telecomunicació*
Àrea del Treball Final:	*Administració de xarxes y Sistemes Operatius*
Idioma del treball:	*Català*
PARAULES CLAU:	*Ciberseguretat, ciberatac, ISO*

RESUM DEL TREBALL:

La ciberseguretat, en informàtica, és un terme que es refereix a les diverses mesures d'un sistema informàtic, independentment si es tracta d'un únic ordinador o d'una xarxa interconnectada, orientades a protegir-lo dels ciberatacs o qualsevol mena de ciberincident que pugui ser causat des de l'exterior, habitualment mitjançant Internet.

Un cop definit el camp de recerca, la meva voluntat és fer un treball que estudiï detalladament l'aplicació de les normatives ISO o BS7799 de seguretat, que fan que l'estructura informàtica de qualsevol empresa passi per un procés de canvi estructural important. L'objectiu principal és millorar i garantir la correcta aplicació d'aquestes normatives contemplant tots els aspectes dins de l'àmbit informàtic i legal.

Després de veure les dificultats que pot tenir qualsevol petita o mitjana empresa per a implementar tota la normativa vigent per a protegir-se davant de qualsevol ciberatac. Vaig creure oportú crear una guia per tal d'aconsellar en les primeres accions i ajudar a les empreses que per algun tipus de motiu no disposen dels recursos suficients per a modernitzar o contractar els serveis integrals a una empresa externa amb l'elevat cost que això suposa. Aquesta guia vol suposar un canvi en la manera de com qualsevol petita o mitjana empresa pot fer el pas per a protegir-se d'una forma segura tot complint amb la normativa vigent.

ABSTRACT:

Cybersecurity in computer science refers to the various measures of a computer system, regardless of whether it is a single computer or an interconnected network, aimed at protecting it from cyberattacks or any kind of cyberincident that may be caused from the outside, usually via the Internet.

Once the field of research is defined, my will is to carry out a work that will study in detail the application of the ISO or BS7799 safety regulations, which make the computer structure of any company undergo a major structural change process. The main objective is to improve and ensure the correct application of these regulations by taking account of all aspects within the computer and legal field.

So, having seen the difficulties that any small or medium-sized enterprise may have in implementing all the existing regulations to protect itself against any cyberattack. I felt it appropriate to create a guide to advise on early actions and help companies that for some reason do not have sufficient resources to modernise or hire full services to an external company at the high cost. This guide aims to change the way in which any small or medium-sized enterprise can take the step of protecting itself in a safe manner while complying with the current rules.

Índex d'Ilustracions

Índex de Taules

1. Introducció

1.1. Context

En l'era digital en la qual vivim, on la tecnologia es troba present i juga un paper clau en pràcticament tots els aspectes de les nostres vides, la ciberseguretat ha esdevingut una preocupació de summa importància.

Cal fer esment que la creixent interconnexió de dispositius i sistemes informàtics ha creat una multitud de desafiaments relacionats amb la protecció de la informació i les infraestructures crítiques contra les diferents amenaces cibernètiques a les quals estem exposats. Els ciberatacs, els podem entendre com qualsevol mena d'intent de caràcter maliciós amb l'objectiu de comprometre la integritat, confidencialitat o disponibilitat dels sistemes i dades, representen una realitat omnipresent en la nostra societat actual.

És ben cert que l'evolució de les tecnologies de la informació i la comunicació (TIC) ha aportat innombrables beneficis a la societat, però alhora ha obert noves portes per als delinqüents cibernètics.

Els ciberatacs poden variar en la seva naturalesa i complexitat, des d'atacs d'enginyeria social i malware fins a atacs de denegació de servei distribuït, el que es coneix amb les sigles (DDoS), o fins i tot, violacions de dades a gran escala. Aquests tipus d'amenaces no només afecten les persones de forma individual, sinó també a governs, organitzacions i empreses de totes les grandàries, causant pèrdues econòmiques importants així com danys vers la reputació.

La ciberseguretat s'ha convertit en un camp en constant evolució, en el qual professionals i experts en seguretat informàtica es dediquen a desenvolupar estratègies, eines i polítiques per a mitigar els riscos associats amb els ciberatacs. La implementació efectiva de les mesures de seguretat cibernètica esdevé essencial per a garantir la privacitat de la informació personal, protegir els actius digitals i salvaguardar la infraestructura crítica.

A més a més, el panorama de la ciberseguretat es veu influenciat per noves tendències tecnològiques, com la intel·ligència artificial, la computació en el núvol o l'Internet of Things (IoT).

Les noves tendències presenten al mateix temps oportunitats com desafiaments addicionals en la protecció de les dades i els sistemes. La col·laboració entre els sectors públic i privat, la conscienciació dels usuaris i l'adopció de millors pràctiques de seguretat són fonamentals per a fer front a la creixent sofisticació dels ciberatacs i enfortir la resiliència en el ciberespai.

2. Antecedents

2.1. Estat de la qüestió

La ciberseguretat busca protegir els sistemes, xarxes i dades de les amenaces cibernètiques. A mesura que la tecnologia avança i les tècniques d'atac es tornen més sofisticades, és essencial comprendre l'estat actual de la ciberseguretat i les tendències en aquest camp.

Un dels avenços més destacats en món de la ciberseguretat és l'aplicació de tècniques d'intel·ligència artificial (IA) i aprenentatge automàtic (*machine learning*). Aquestes tècniques s'usen per a desenvolupar sistemes de detecció i resposta en temps real. Les tècniques esmentades permeten d'analitzar grans volums de dades i reconèixer patrons anòmals que podrien indicar un atac en curs. La intel·ligència artificial també s'aplica en la identificació de vulnerabilitats en els sistemes i en la millora de la resposta davant dels incidents.

Un altre aspecte important és l'adopció d'enfocaments de seguretat centrats en el núvol. Amb la creixent migració dels serveis en el núvol, s'han desenvolupat solucions de seguretat específiques per a protegir les dades i les aplicacions en entorns de computació en el núvol. Això inclou el xifratge de dades, l'autenticació multifactor i el monitoratge constant per a detectar activitats sospitoses.

La ciberseguretat també ha experimentat avenços en la detecció i prevenció d'atacs d'enginyeria social. Els ciberdelinqüents cada vegada més fan ús de tècniques d'enginyeria social, com el phishing i el spear phishing, per a enganyar els usuaris i obtenir accés a informació confidencial. En resposta a això, s'han desenvolupat solucions de conscienciació i prevenció per a dotar als usuaris de la informació necessària per a reconèixer i evitar aquest tipus d'atacs.

La col·laboració i l'intercanvi d'informació entre els diversos actors de la ciberseguretat també ha millorat en els últims anys. Tant a escala nacional com internacional, s'han establert iniciatives i organismes especialitzats a compartir informació sobre amenaces, tàctiques i tècniques d'atacs. D'aquesta manera, s'aconsegueix una resposta més ràpida i coordinada enfront dels ciberatacs, i contribueix a enfortir la resiliència de les organitzacions i les infraestructures crítiques.

A més a més, la protecció de la privacitat de les dades i el compliment normatiu han guanyat major importància en l'àmbit de la ciberseguretat. Les regulacions, com el Reglament General de Protecció de Dades (RGPD) a la Unió Europea, estableixen requisits estrictes per a la protecció de les dades personals. Les organitzacions han d'implementar mesures tècniques i organitzatives per a garantir la privacitat i complir amb les regulacions aplicables.

Així doncs, la ciberseguretat mostra avenços significatius en àrees com la intel·ligència artificial o la seguretat en el núvol entre els actors de la ciberseguretat. Caldrà fer una correcta aplicació d'aquestes tecnologies per tal d'enfortir la protecció dels sistemes i dades, sense deixar de banda la importància de la conscienciació dels usuaris i el compliment normatiu per a una estratègia integral de ciberseguretat.

3. Propòsits i objectius

3.1. Motivació del projecte

La idea de fer aquest treball, tot i que ha evolucionat amb el pas del temps, va ser introduïda per la meva tutora del Treball Final de Grau, Arianna Arlet Garrido Blanes, enginyera Informàtica juntament amb els companys i companyes de l'empresa on actualment treballo, NTT Data.

Després d'hores de conversa relacionades amb el món tecnològic i, en especial, de tot el que envolta el món de la ciberseguretat em vaig adonar que hi havia un buit per a les petites i mitjanes empreses en el moment d'aplicar tota la normativa vigent.

Des d'un punt de vista més personal, vaig decidir endinsar-me en el món de la ciberseguretat, ja que vaig començar a entreveure el meu futur professional i les possibilitats que aquest món ofereix. Sempre m'ha agradat ser capaç de resoldre les coses de la manera més eficient, per tal que siguin més senzilles, ràpides i donin més prestacions.

Tal com afirmava el cèlebre filòsof Aristòtil, "*La intel·ligència no només consisteix en el coneixement, sinó també en la destresa d'aplicar els coneixements a la pràctica*".

Amb aquest treball començo un repte personal analitzant un problema actual i intentant trobar solucions per tal de posar la tecnologia al servei de qualsevol petita empresa que hagi de fer el canvi en l'àmbit de l'estructura informàtica per aplicar les normatives ISO o la normativa BS7799. Tinc consciència que la tecnologia i les normatives evolucionen i que em caldrà aprendre de forma ininterrompuda al llarg de la meva vida.

3.2. Objectius del projecte

Avui en dia Internet ha canviat del tot la nostra percepció de la realitat i la manera de relacionar-nos amb l'entorn.

Els experts ja afirmen que aquest mateix any el nombre de ciberatacs creixerà de forma exponencial. Per tant, caldrà que qualsevol individu o institució prengui mesures per tal de

protegir-se. Des de l'àmbit empresarial també implica que cada cop les organitzacions hagin de destinar més recursos per a protegir-se vers qualsevol possible atac.

Així doncs, el primer objectiu del meu projecte serà el de proporcionar una idea sòlida i concreta de tot el que envolta les normatives ISO o BS7799 de seguretat aquesta darrera. És a dir, estudiar a fons la normativa ISO, gestió integral.

El segon objectiu, recau en la investigació de com s'aplica actualment aquestes normatives en diferents tipus d'empreses. Em centraré, especialment, en les petites i mitjanes empreses tot i que també s'analitzarà el cas de les grans empreses per poder veure les principals diferències.

Per la meva motivació personal, i alhora per fer un projecte més rigorós he cregut oportú presentar una guia de com aplicar les normatives ISO o BS7799 amb la intenció de millorar-ne la implementació actual, convertint-se aquest en l'objectiu principal de la meva recerca.

D'aquesta manera i a partir de l'esmentat anteriorment podem establir tres objectius específics:

- Conèixer de manera detallada les normatives ISO, gestió integral o la normativa BS7799 tant en l'àmbit teòric com tècnic.

- Investigar la seva implementació actual en els diferents tipus d'empreses tenint en compte els seus pros i contres.

- Presentar una guia d'aplicació de les normatives esmentades per a les petites i mitjanes empreses.

4. Abast del projecte

L'abast d'aquest projecte s'enfoca en la creació d'una guia pràctica i teòrica que ajudi a les petites empreses en l'assesorament i futur desplegament de les normatives ISO 27001 i ISO 27002, amb la finalitat d'enfortir la seguretat de la informació.

El projecte comprendrà les següents activitats:

1. Anàlisi i avaluació de les necessitats de seguretat de la informació de les empreses: Es farà una anàlisi de les necessitats de les empreses per a comprendre els seus requisits i desafiaments específics en termes de ciberseguretat.

2. Desenvolupament de la guia pràctica i teòrica: A partir de la informació recollida en l'anàlisi, es desenvoluparà una guia completa que proporcioni a les empreses els coneixements i les millors pràctiques necessàries per a implementar les normatives ISO 27001 i ISO 27002 de manera efectiva. La guia inclourà explicacions teòriques, exemples pràctics i recomanacions per a la implementació.

3. Validació de la guia: La guia serà verificada per experts en ciberseguretat per a assegurar la seva qualitat i precisió. Es duran a terme revisions i ajustos necessaris per a garantir que la guia sigui clara, completa i aplicable a diferents escenaris empresarials.

Fora de l'àmbit de l'elaboració d'aquest treball i per a la futura utilitat i continuïtat de la guia també serà rellevant dur a termes dos punts més:

4. Distribució i difusió de la guia: Una vegada validada, la guia serà distribuïda i difosa entre les empreses interessades a millorar la seva seguretat de la informació. S'utilitzaran diferents canals de comunicació, com a llocs web, seminaris i esdeveniments especialitzats, per a aconseguir arribar a un ampli públic empresarial.

5. Seguiment i actualització de la guia: S'establirà un mecanisme de seguiment i retroalimentació per a recopilar comentaris de les empreses que usin la guia. Aquests comentaris seran usats per a millorar i actualitzar periòdicament la guia, assegurant així la seva rellevància i utilitat contínua.

Cal destacar que l'objectiu final del treball de fi de grau és proporcionar a les empreses una guia pràctica i teòrica que els permeti enfortir la seva seguretat de la informació i complir amb els estàndards establerts per les normatives ISO 27001 i ISO 27002.

En resum, l'abast del projecte se centra en el desenvolupament d'una guia teòrica i pràctica que ajudi a les empreses en la implementació de les normatives ISO 27001 i ISO 27002.

5. Eines i recursos

Per la realització d'aquest Treball Final de Grau es faran servir diferents recursos i eines que ajudaran en la recerca de la informació així com en l'elaboració de la memòria entre altres.

Primerament, en la fase inicial del projecte es faran servir diverses eines que ajudin en la recerca de la informació. Algunes d'aquestes eines són la biblioteca de la UOC, ResearchGate o Google Scholar amb la finalitat de trobar articles de caràcter acadèmic. A més a més, es faran consultes sobre la normativa ISO o la normativa BS7799. També, es faran consultes al BOE i d'altres organismes Europeus amb la finalitat de consultar més àmpliament la normativa vigent. A banda d'això, també es consultarà el pla de desplegament i aplicació de les normatives esmentades en les grans empreses.

En relació amb l'àmbit d'edició, es farà servir l'eina Pages per l'elaboració de la memòria. D'altra banda, també es faran servir recursos de Google com Google Drive o les eines Gmail o Meet per mantenir el contacte constant amb la tutora d'aquest projecte. Més enllà de les aplicacions de Google, també es farà servir l'eina OpenProject per la realització del diagrama de Gantt.

En la segona fase, centrada més en la part de desenvolupament de la memòria així com de recollida i selecció de tota la informació trobada. Es faran servir les eines que siguin necessàries esmentades en la primera fase.

Finalment, per l'elaboració de la presentació virtual, s'utilitzarà algun programari, encara per definir, per tal de fer la gravació i l'edició del vídeo final. A més a més, d'alguna eina, possiblement Keynote o alguna aplicació semblant per la creació d'un document on poder presentar de forma sintetitzada tota la recerca feta.

6. Planificació

6.1. Enfocament

En aquest Treball de Fi de Grau, l'enfocament adoptat es centra en el desenvolupament d'una guia teòrica i pràctica per a ajudar a les empreses en el correcte desplegament de les normatives ISO 27001 i ISO 27002, amb l'objectiu d'enfortir la seva seguretat de la informació. Tot seguit es fa un breu descripció de la metodologia seguida durant el desenvolupament del treball:

En primer lloc, la revisió i anàlisi de les normatives: S'ha dut a terme una exhaustiva revisió bibliogràfica per a familiaritzar-se amb els conceptes clau de la seguretat de la informació i comprendre detalladament les normatives ISO 27001 i ISO 27002. També, s'han analitzat els requisits i recomanacions establerts en aquestes normatives així com les millors pràctiques possibles.

En segon lloc, la identificació de les necessitats empresarials: S'ha intentat comprendre al màxim les necessitats de les empreses, especialment les de mida més petites, per tal de conèixer les seves necessitats específiques en termes de seguretat de la informació. A partir de la investigació feta, s'han recopilat dades clau amb relació als principals desafiaments als quals s'enfronten les empreses en la implementació de les normatives ISO, així com les seves expectatives i requisits particulars.

En tercer lloc, el desenvolupament de la guia: Amb base en la revisió i l'anàlisi de normatives, s'ha procedit al desenvolupament de la guia teòrica i pràctica. S'ha estructurat la guia de manera clara i senzilla, abordant els aspectes més rellevants de la implementació de les normatives ISO 27001 i ISO 27002. Per tal d'assolir aquest propòsit, s'han inclòs explicacions teòriques, exemples pràctics i recomanacions per a facilitar la implementació.

Finalment, també seria interessant dur a terme el punt que es descriu a continuació. Malgrat això, en el desenvolupament d'aquest Treball Final de Grau no s'ha implementat pel fet que quedava fora de l'abast del projecte.

Proves pilot i retroalimentació: Seria rellevant, de cara a la implementació i utilitat de la guia seleccionar diferents empreses per a dur a terme proves pilot de la guia. A partir de les proves pilot, caldria recopilar la retroalimentació d'aquestes empreses, avaluant la

seva experiència en la implementació de les normatives ISO utilitzant la guia desenvolupada. Aquesta retroalimentació seria emprada per a realitzar millores finals en la guia abans de la seva distribució final.

6.2. Planificació general del projecte

La planificació general d'aquest projecte ve determinat a partir de quatre entregues parcials del contingut per acabar creant l'estructura del projecte final. Dites entregues parcials, estan definides d'acord amb el calendari lectiu de l'assignatura de la següent forma:

Data límit	Entregable
19/03/2023	PAC1 - Proposta de pla de treball
23/04/2023	PAC2 - Entrega de l'entre el 40% i el 60% de tot el TFG
28/05/2023	PAC3 - Entrega de l'entre el 80% i el 90% de tot el TFG
18/06/2023	Entrega Final: Memòria i presentació

Taula 01 - Entregables durant la realització del TFG. (Elaboració pròpia)

A partir de la taula anterior, podem considerar cada data límit com un *milestone* a assolir. Així doncs, podrem crear la planificació global de tot el projecte per tal d'assolir els objectius plantejats anteriorment en aquest document.

Cal destacar que per tal de fer la distribució de les diferents tasques he considerat que tots els dies són hàbils de cara a l'execució de les tasques relacionades amb el projecte. D'aquesta manera, s'aconsegueix disposar de petits espais de temps addicionals per a possibles entrebancs que puguin sorgir al llarg de l'elaboració del projecte.

A continuació, es presenta una taula amb la descomposició de tasques dutes a terme al llarg del projecte.

Entrega	Data Entrega	Fita	Data Inici	Data fi
PAC 1	19/03/2023	Proposta del Projecte	01/03/2023	18/03/2023
		Introducció i Antecedents	01/03/2023	04/03/2023
		Propòsits i Objectius	05/03/2023	08/03/2023
		Abast del Projecte i Eines	10/03/2023	12/03/2023
		Planificació i Metodologia del Treball	13/03/2023	16/03/2023
		Entrega PAC 1	16/03/2023	19/03/2023
PAC 2	23/04/2023	Desenvolupament i execució del projecte PAC 2	20/03/2023	22/04/2023
		Revisió de les normatives ISO	21/03/2023	24/03/2023
		Desenvolupament guia, àmbit teòric	21/03/2023	19/04/2023
		Introducció i Història del món de la ciberseguretat	22/03/2023	24/03/2023
		Normativa legislativa de la ISO	25/03/2023	28/03/2023
		Marc teòric de la normativa ISO	28/03/2023	31/03/2023
		Introducció i Descripció de la família ISO 27000	01/04/2023	19/04/2023
		Desenvolupament: ISO 27001, ISO 27002, ISO 27003	02/04/2023	07/04/2023
		Desenvolupament: ISO 27004, ISO 27005	08/04/2023	12/04/2023
		Desenvolupament: ISO 27006 i BS7799	13/04/2023	18/04/2023
		Identificació de les necessitats empresarials	18/04/2023	23/04/2023
		Revisió entregable PAC 2 i altres detalls	20/04/2023	22/04/2023
		Entrega PAC 2		23/04/2023
PAC 3	28/05/2023	Desenvolupament i execució del projecte PAC 3	24/04/2023	27/05/2023
		Revisió de les propostes de millora PAC 2	25/04/2023	27/04/2023
		Desenvolupament guia, àmbit pràctic	27/04/2023	25/05/2023
		Orientacions per a l'empresa i Aspectes Clau	27/04/2023	30/04/2023
		Aplicació normativa ISO 27000	01/05/2023	03/05/2023
		Consideracions en relació amb l'ISO 27001	04/05/2023	06/05/2023
		Consideracions en relació amb l'ISO 27002	06/05/2023	08/05/2023
		Aplicació per a les PIME	09/05/2023	12/05/2023
		Estructura ISO 27001 i ISO 27002	12/05/2023	18/05/2023
		Preguntes Freqüents	19/05/2023	20/05/2023
		Revisió i validació de la guia	20/05/2023	24/05/2023
		Revisió entregable PAC 3 i altres detalls	25/05/2023	27/05/2023
		Entrega PAC 3		28/05/2023
Entrega Final	18/06/2023	Desenvolupament tasques finals TFG	29/05/2023	17/06/2023
		Revisió de les propostes de millora PAC 3	30/05/2023	02/06/2023
		Redacció conclusions finals	03/06/2023	08/06/2023
		Redacció Glossari	04/06/2023	06/06/2023
		El·laboració final bibliografia	06/06/2023	07/06/2023
		Revisió Memòria final	10/06/2023	16/06/2023
		El·laboració presentació TFG	05/06/2023	12/06/2023
		Gravació presentació TFG	15/06/2023	16/06/2023
		Revisió final entregables i altres detalls	16/06/2023	17/06/2023
		Entrega final Memòria TFG		18/06/2023

Taula 02 - Taula resum de les dates principals del projecte. (Elaboració pròpia)

6.3. Viabilitat tecnològica del projecte

La viabilitat tecnològica del projecte és alta des del punt de vista de la implementació de l'ISO i altres normatives de ciberseguretat. L'ISO (Organització Internacional de Normalització) proporciona un marc de treball àmpliament acceptat per gestionar la seguretat de la informació. Les normatives relacionades, com ara l'ISO 27001 i l'ISO 27002, estableixen requisits i recomanacions per a l'establiment, implementació i millora continuada d'un sistema de gestió de la seguretat de la informació (SGSI).

L'objectiu de la guia és proporcionar orientació teòrica i pràctica per a les empreses petites posant a l'abast els elements bàsics de la informació ja existent a partir de les grans empreses amb implementacions existents.

Per a la implementació de l'ISO i altres normatives, es disposarà de recursos com guies i documents orientatius proporcionats per l'organització ISO i altres fonts fiables. Això permetrà dur a terme una anàlisi exhaustiva de les necessitats de seguretat de la informació de les empreses, identificar les seves vulnerabilitats i implementar les mesures de seguretat adequades.

La infraestructura en el núvol també pot jugar un paper important en la viabilitat tecnològica del projecte, proporcionant un entorn escalable i flexible per a l'emmagatzematge i processament de dades relacionades amb la seguretat de la informació. Això permetrà als responsables de la seguretat gestionar de manera eficient les polítiques, procediments i controls necessaris per a la conformitat amb les normatives establertes.

En resum, tenint en compte les tecnologies i recursos disponibles, així com l'ús d'infraestructura en el núvol i la col·laboració amb experts en ciberseguretat, es conclou que la viabilitat tecnològica del projecte és prometedora i que es disposa de les eines necessàries per a l'elaboració d'una guia eficaç i pràctica per a les empreses en el desplegament de l'ISO.

7. Metodologia de treball

El present Treball de Fi de Grau s'ha desenvolupat seguint una metodologia que combina diferents etapes i enfocaments per a aconseguir els objectius proposats. S'ha dut a terme un enfocament mixt, és a dir, s'ha combinat tant elements quantitatius com qualitatius.

A continuació, es detalla la metodologia de treball seguida al llarg d'aquest projecte:

1. Revisió i anàlisi de normatives:

    1.1. Realitzar una revisió exhaustiva tècnica relacionada amb la seguretat de la informació, la normativa ISO 27001 i ISO 27002, així com les millors pràctiques en ciberseguretat.

    1.2. Analitzar detalladament els requisits i recomanacions establerts en les normatives ISO, identificant els aspectes bàsics per a la implementació d'un sistema de gestió de la seguretat de la informació (SGSI).

2. Identificació de les necessitats empresarials:

    2.1. Dur a terme entrevistes a empreses per a comprendre les seves necessitats pel que fa a la seguretat de la informació.

    2.2. Recollir la informació sobre les vulnerabilitats comunes, els riscos percebuts i les expectatives de les empreses en relació amb la implementació de les normatives ISO.

3. Definició de l'abast del projecte:

    3.1. Establir els límits i l'enfocament específic del projecte, centrant-se d'una forma clara en el desenvolupament d'una guia pràctica i teòrica per a ajudar a les empreses en la implementació de les normatives ISO corresponents.

4. Desenvolupament de la guia:

    4.1. Elaborar una guia estructurada que abordi els aspectes essencials de la implementació de les normatives ISO, incloent-hi explicacions teòriques, exemples pràctics i recomanacions.

4.2. Garantir que la guia sigui clara i de fàcil comprensió per a les empreses.

5. Validació de la guia:

5.1. Sotmetre la guia desenvolupada a la revisió d'un expert en en el camp de la ciberseguretat. Recopilar comentaris, suggeriments i millores proposades per integrar-ho a la guia.

6. Avaluació de resultats:

6.1. Analitzar els resultats obtinguts avaluant la guia en la implementació de les normatives ISO en les empreses.

6.2. Comparar els resultats amb els objectius plantejats inicialment, identificant possibles àrees de millora i recomanacions per a futures recerques.

En conclusió, aquesta metodologia de treball ha de permetre desenvolupar un Treball Final de Grau centrat en la creació d'una guia teòrica i pràctica per a ajudar a les empreses en la implementació de les normatives ISO. La metodologia plantejada ha de permetre abordar de manera integral els objectius del projecte i garantir la utilitat de la guia.

8. Guia: Implementació de la ISO gestió integral, en una petita empresa

8.1. Introducció al món de la ciberseguretat

Aquesta guia vol començar amb una breu introducció en el món de la ciberseguretat per ajudar a entendre els conceptes més importants que envolten aquesta paraula que en l'actualitat podem escoltar cada dia de forma recurrent.

La necessitat de crear aquesta guia va més enllà de la creació d'una sèrie de passos a seguir, si no que vol crear un impacte positiu a qualsevol persona que la llegeixi amb la finalitat d'ajudar-la a entendre i poder crear d'una forma clara i entenedora tot el que envolta el concepte de ciberseguretat.

Podem definir la ciberseguretat com el conjunt de tècniques, pràctiques i mesures preventives que es posen en pràctica amb l'objectiu de protegir les xarxes, els sistemes informàtics i, fins i tot, qualsevol dispositiu que es pugui connectar a la xarxa. És a dir, pel simple fet de tenir accés a la xarxa qualsevol dispositiu es converteix en vulnerable i passar a estar exposat a poder rebre alguna mena d'atac per tal d'explotar-ne les vulnerabilitats.

Per tant, la ciberseguretat té un repte majúscul. El de protegir tota la informació digital de qualsevol atac de caràcter sospitós o malintencionat, així com d'una possible interrupció de qualsevol servei de la xarxa o dels sistemes crítics fins a la possible usurpació de les dades.

Tal com va afirmar el cèlebre Eugene Howard Spafford, professor americà d'informàtica a la Universitat de Purdue i expert en seguretat informàtica: "*El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de concreto, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él*".

8.2. Història de la ciberseguretat

La ciberseguretat, tal com s'ha explicat anteriorment, és un camp de la informàtica que s'encarrega de protegir els sistemes informàtics i les xarxes contra les possibles amenaces cibernètiques. La ciberseguretat és essencial en l'era digital actual per a protegir la confidencialitat, integritat i disponibilitat de la informació digital i garantir la privacitat i seguretat tots els usuaris que es troben a la xarxa.

Cal destacar que la ciberseguretat com a disciplina no té una data de naixement exacta, ja que la seva evolució s'ha anat produint gradualment amb el desenvolupament de la tecnologia informàtica.

La història de la ciberseguretat es remunta a la dècada de 1950, quan els primers sistemes informàtics i xarxes van començar a sorgir. En aquell moment, la seguretat se centrava principalment en la protecció a escala física dels equips i dispositius. Algunes de les tècniques que s'aplicaven eren la implementació de panys o altres dispositius de seguretat per a evitar el robatori i la manipulació no autoritzada dels sistemes.

Amb l'evolució ininterrompuda de la tecnologia, els atacs cibernètics també han canviat convertint-se en cada cop atacs més perillosos i sofisticats. A principis dels anys vuitanta, el primer virus informàtic, anomenat "Elk Cloner", va ser descobert en una màquina d'Apple II. Es pot considerar el primer virus, ja que fou el primer a tenir una expansió real i no es trobava emmarcat com una prova de laboratori. Aquell virus es va propagar a través de disquets i va marcar el començament d'una era d'amenaces cibernètiques cada vegada més elaborades.

A mesura que les organitzacions i empreses van començar a utilitzar cada vegada més la tecnologia informàtica, es va fer evident que era vital implementar noves mesures de seguretat per a protegir els sistemes i les dades. Més endavant, als anys noranta van sorgir els primers tallafocs i sistemes de detecció d'intrusions (IDS) per a ajudar a protegir les xarxes.

Una altra data clau va ser l'aparició de World Wide Web (www.) en la dècada de 1990, quan l'amenaça dels atacs cibernètics es va tornar encara més greu. Els llocs web van esdevenir el focus dels ciberdelinqüents i els atacs de denegació de servei (DDoS) es van tornar cada vegada més comuns. En aquest context, van sorgir noves tècniques de seguretat, com la criptografia i l'autenticació d'usuaris, per tal de protegir els llocs web així com tota la informació que contenen.

En la dècada dels 2000, es va produir un augment dramàtic en els atacs cibernètics i es va fer evident la necessitat d'una estratègia integral de ciberseguretat. A mesura que els atacs es van tornar més sofisticats, també ho van fer les tècniques de defensa. Avui dia, amb atacs viscuts de forma recent a universitats o hospitals, entre altres, la ciberseguretat esdevé una prioritat per tal de protegir-se i fer front als atacs amb finalitats malintencionades.

En resum, la ciberseguretat ha evolucionat significativament juntament amb la tecnologia al llarg dels anys fins a arribar a ser cada vegada més rellevant per fer front a la gran quantitat d'atacs que es cometen avui en dia. Al llarg d'aquests setanta anys aproximadament, s'han produït una gran varietat d'innovacions i avanços tecnològics en l'àmbit de la informàtica i les telecomunicacions. Per tant, mentre que l'evolució i la innovació de les tecnologies ha dotat a la societat de noves eines per comunicar-se o fer negocis entre altres, també ha suposat la creació de noves amenaces i reptes de seguretat.

S'estima que la mitja de ciberatacs diaris és 2.200 atacs cibernètics al dia, el que vol dir que es produeix un atac cibernètic cada 39 segons de mitjana. Aquesta xifra representa que a l'any es produeixen de mitjana uns 800.000 ciberatacs. D'acord amb l'article titulat *"How Many Cyber Attacks Happen Per Day in 2023?"* escrit per Jacquelyn Bulao, algunes de les dades més rellevants i curioses són:

- Cada 39 segons hi ha un nou atac hacker.
- Cada dia es creen al voltant de 300.000 programaris maliciosos nous.
- L'assistència sanitària és el principal objectiu dels atacs on es demana un rescat.
- El 92% del programari maliciós es lliura mitjançant el correu electrònic.
- 4,1 milions de llocs web tenen programari maliciós en qualsevol moment.
- Quaranta-nou dies és el temps mitjà que es triga a identificar un atac on es sol·licita un rescat.
- El 97% de totes les filtracions de seguretat exploten les extensions del WordPress.

- Fins ara s'han robat aproximadament tres mil milions de dòlars de criptomoneda mitjançant atacs.

- El 66% dels CIO (Chief Information Officer) asseguren que tenen previst augmentar la inversió en ciberseguretat.

Avui en dia, la ciberseguretat té un impacte crític en el món en el qual vivim. En l'era digital en la qual la majoria dels serveis i transaccions es duen a terme a través de la xarxa, la seguretat de la informació digital és essencial per a garantir la privacitat i protecció de les dades personals dels usuaris i la integritat dels sistemes informàtics i xarxes.

Qualsevol amenaça cibernètica esdevé una preocupació important, i alhora una prioritat, per a empreses, organitzacions i governs d'arreu del món, per tal de protegir els seus sistemes informàtics i prevenir atacs malintencionats que poden desencadenar conseqüències molt greus. Més enllà de voler protegir o prevenir possibles atacs, la ciberseguretat juga un paper clau, ja que és essencial per a garantir la continuïtat dels serveis considerats com a crítics. És a dir tots aquells serveis vitals com els serveis de salut, financers i governamentals, entre altres, que depenen d'una forma molt notable de la tecnologia informàtica i les xarxes.

8.3. Normativa legislativa de la ISO, gestió integral

La normativa legislativa de l'ISO fa referència al conjunt de normes establertes per l'Organització Internacional de Normalització (ISO, per les seves sigles en anglès) per a establir tots els requisits, les directrius i els estàndards en diferents àmbits, amb el principal objectiu de promoure la qualitat, la seguretat i l'eficiència en diferents sectors.

L'Organització Internacional de Normalització, és una entitat totalment independent que desenvolupa i promou els estàndards internacionals en una àmplia varietat d'àrees, inclosa la gestió integral.

Convé destacar que l'ISO (*International Organization for Standardization*) fou creada l'any 1947. El terme ISO prové del grec "isos" on el seu significat és "igual". Malgrat això, s'usa únicament el terme ISO en lloc d'ISO / IEC per qüestions de simplicitat. La gestió integral es refereix a un enfocament holístic per a administrar una organització de manera integrada, considerant aspectes com la qualitat, el medi ambient o la salut entre altres. Més enllà de l'ISO relacionada amb el món de la ciberseguretat, també existeixen altres normatives legislatives relacionades amb la gestió integral en diferents àrees. Algunes d'aquestes altres ISO són les següents:

- ISO 9001:2015

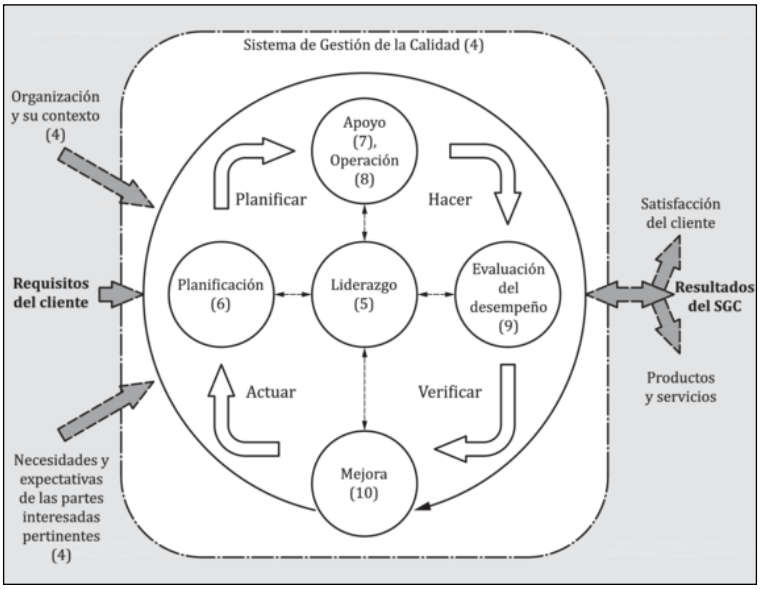
És l'última versió de la norma ISO 9001 per a sistemes de gestió de la qualitat. Es tracta d'un conjunt de directrius i requisits perquè les organitzacions implementin un sistema de gestió de la qualitat (SGC) que garanteixi que satisfacin de manera consistent les necessitats i expectatives dels clients.

La norma és aplicable a organitzacions de totes les grandàries en qualsevol indústria o sector. En implementar ISO 9001:2015, les organitzacions poden millorar les seves pràctiques de gestió de qualitat, millorar la satisfacció del client i augmentar en certa manera la competitivitat en el mercat.

La certificació ISO 9001:2015 no és obligatòria, però moltes organitzacions decideixen obtenir-la com una manera de demostrar el seu compromís amb la qualitat i diferenciar-se dels competidors. Per tal d'assolir la certificació cal superar una auditoria externa del SGC

d'una organització per a garantir que es compleix amb els requisits de la norma ISO 9001:2015.

D'acord amb la Norma Internacional, en la següent il·lustració, es mostra el cicle PHVA (Planificar - Hacer - Verificar - Actuar). En concret, la il·lustració presenta com es poden agrupar els capítols del quatre al deu d'acord amb el cicle PHVA.



Il·lustració 01 - Representació de l'estructura de la Norma ISO 9001:2015 amb el cicle PHVA. (ISO 9001:2015)

Nota: Els números entre parèntesis fan referència als capítols de la Norma ISO

- ISO 26000:2010

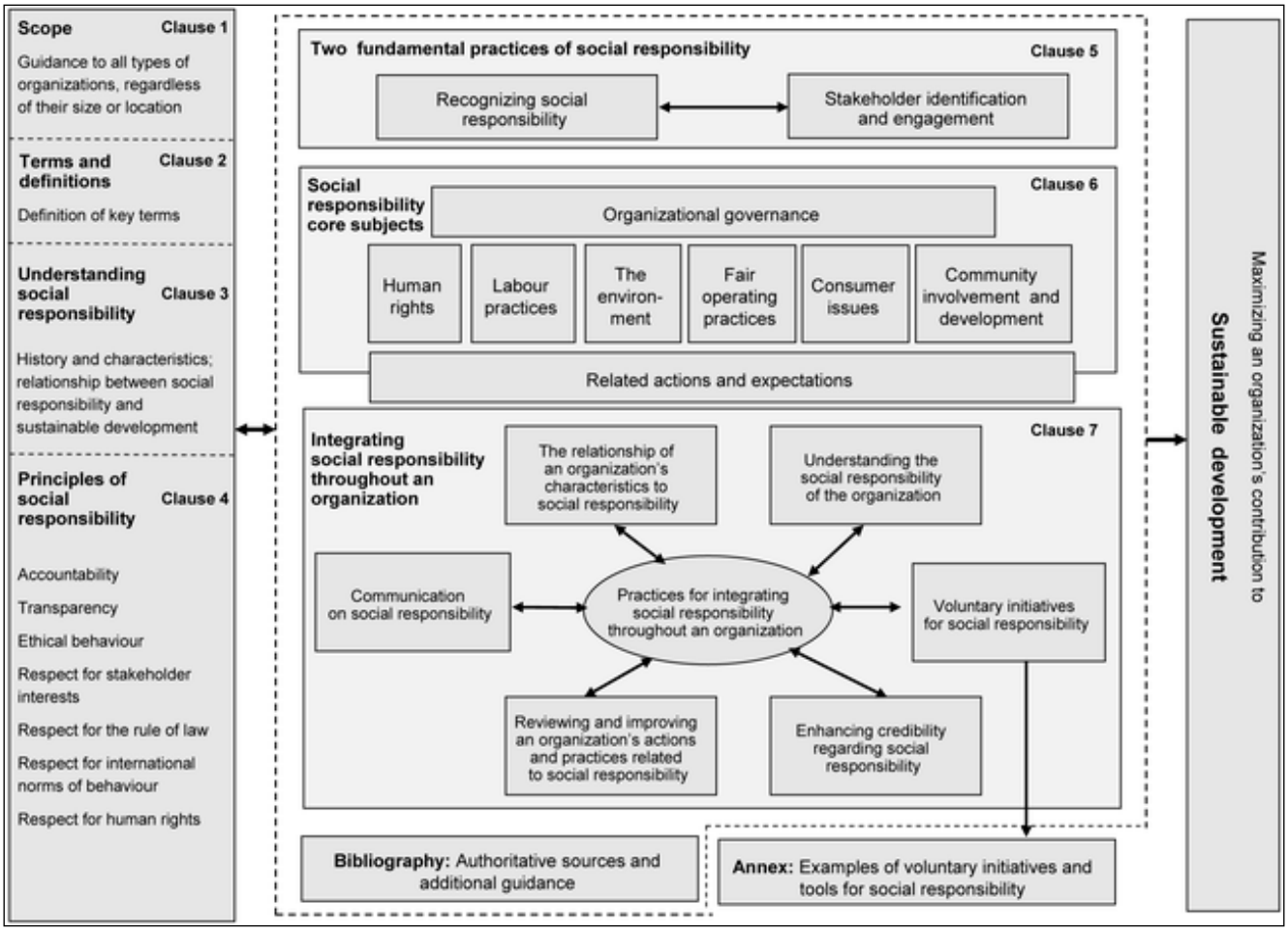
Aquesta norma proporciona directrius per a la responsabilitat social de les organitzacions (RSO). No és una norma de certificació, sinó que ofereix orientació sobre com les organitzacions poden contribuir al desenvolupament sostenible i al benestar de la societat.

ISO 26000:2010 s'aplica a organitzacions de tots els tipus, grandàries i ubicacions geogràfiques. La norma es basa en set principis de responsabilitat social: rendició de comptes, transparència, comportament ètic, respecte als interessos de les parts interessades, respecte a l'estat de dret, respecte als drets humans i respecte al medi ambient.

Les directrius de la norma ISO 26000:2010 se centren en àrees clau de responsabilitat social, que inclouen el govern corporatiu, els drets humans, les pràctiques laborals, el medi ambient, les pràctiques justes d'operació, el desenvolupament de la comunitat i la participació activa i el desenvolupament dels interessats.

Tot i que la certificació no és obligatòria, la implementació dels principis i directrius de la norma ISO 26000:2010 pot ajudar a les organitzacions a millorar la seva reputació o augmentar el seu compromís amb la societat entre altres.

D'acord amb la Norma Internacional, en la següent il·lustració, es mostra una visió general de la Norma ISO 26000 i el seu objectiu és ajudar a les organitzacions a comprendre com utilitzar aquesta Norma.



Il·lustració 02 - Representació esquemàtica de la Norma ISO 26000. (ISO 26000)

- ISO 37001:2016

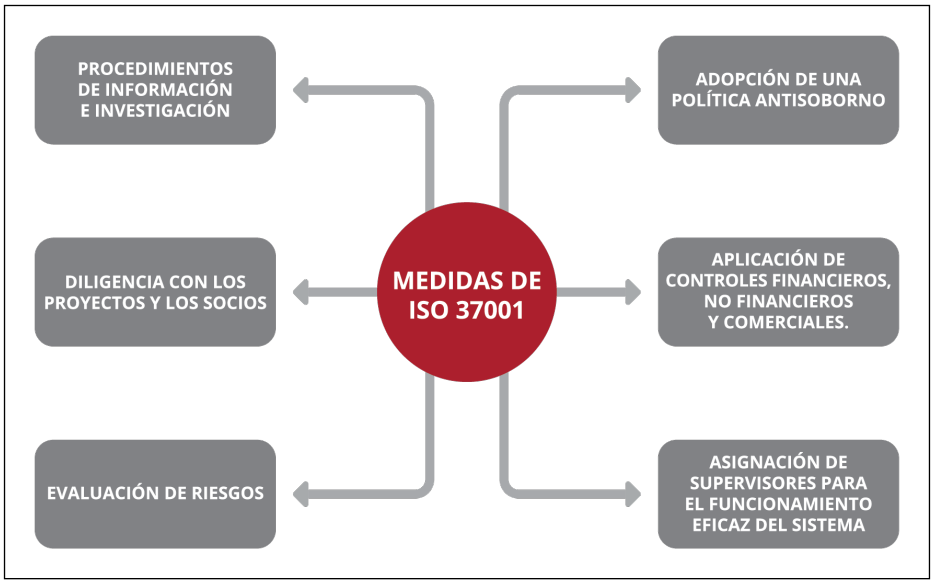
Aquesta norma proporciona directrius i requisits per a un sistema de gestió antisuborn (SGAS). La norma estableix un marc perquè les organitzacions implementin polítiques i procediments efectius per a prevenir, detectar i abordar el suborn en totes les seves formes.

ISO 37001:2016 s'aplica a organitzacions de tots els tipus i en qualsevol sector. Proporciona orientació sobre l'establiment d'una cultura d'ètica i compliment en l'organització, inclosa la formació i sensibilització dels empleats i les parts interessades rellevants.

La norma ISO 37001:2016 estableix requisits per a la implementació d'un SGAS, inclosa l'avaluació de riscos de suborn, la implementació de controls i mesures preventives, la gestió d'incidents i la supervisió i revisió del sistema.

La certificació ISO 37001:2016 no és obligatòria, però pot ajudar les organitzacions a demostrar el seu compromís amb l'ètica i la integritat en les seves operacions comercials. La certificació implica una auditoria de tercers del SGAS de l'organització per a garantir que compleixi amb els requisits de la norma ISO 37001:2016.

D'acord amb la Norma Internacional, en la següent il·lustració, es presenta un esquema amb les principals mesures que ha de dur a terme l'ISO 37001 per a proporcionar les directrius i requisits per a un sistema de gestió antisuborn.



Il·lustració 03 - Representació esquemàtica de les mesures de la Norma ISO 37001. (Intercenter, ISO 37001)

Com hem vist, existeixen multitud de normatives ISO i, per tant, és important destacar que el seguiment i aplicació d'aquestes normes pot variar segons la legislació i regulacions específiques de cada país. Sempre és recomanable consultar la legislació local aplicable i treballar amb experts en l'àrea en qüestió per a garantir la conformitat adequada amb les normatives legislatives i regulacions corresponents en cada cas.

8.4. Marc teòric de la ISO, gestió integral

8.4.1. Introducció

En realitat, no hi ha una sola norma ISO que abordi exclusivament la ciberseguretat. És a dir, existeixen diferents normes ISO que poden ser rellevants per a la gestió de la ciberseguretat. Algunes de les normes ISO més rellevants són:

- ISO 27001 - Sistema de Gestió de Seguretat de la Informació (SGSI)
- ISO 27002 - Codi de pràctica per a la gestió de la seguretat de la informació
- ISO 22301:2019 - Gestió de la continuïtat del negoci
- ISO 31000:2018 - Gestió del risc
- ISO 20000-1:2018 - Gestió de serveis de tecnologia de la informació (TU)

A més a més, també cal destacar la normativa ISO/IEC 27032:2012 que es tracta d'una guia que proporciona un marc per a la ciberseguretat per a la cooperació entre les parts interessades en la gestió de la seguretat cibernètica, incloent-hi el sector privat, el govern i la societat civil.

Així doncs, malgrat que no existeix una única norma ISO específica per a la ciberseguretat, les normes ISO esmentades proporcionen una base prou sòlida per a la gestió de la ciberseguretat en qualsevol mena d'organització.

En el cas que ens ocupa ens centrarem principalment en la família ISO 27000.
La norma central d'aquesta família de normes és l'ISO 27001:2013, que estableix els requisits per a un sistema de gestió de seguretat de la informació. L'ISO 27001 proporciona un marc per a la gestió de la seguretat de la informació en una organització, incloent-hi la identificació de riscos, la selecció i aplicació de controls de seguretat i l'avaluació i millora contínua del sistema.

A més de la norma ISO 27001, hi ha diverses normes addicionals en la família ISO 27000 que poden ser rellevants per a la gestió de la seguretat de la informació:

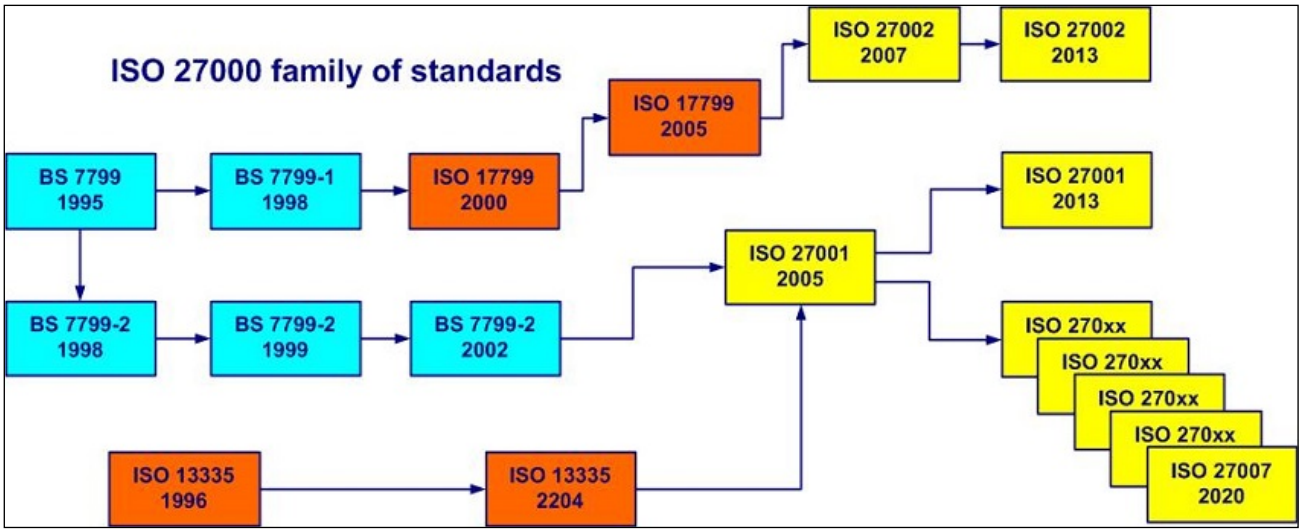
- ISO 27002:2021 - Codi de pràctica per a la gestió de la seguretat de la informació
- ISO 27003:2017 - Guia d'implementació d'un SGSI
- ISO 27004:2016 - Mesurament de l'eficàcia d'un SGSI
- ISO 27005:2018 - Gestió de riscos de seguretat de la informació
- ISO 27006:2015 - Requisits per a la certificació d'un SGSI

8.4.2. Descripció de la familia IS0 27000

Els rangs de numeració reservats per la família ISO 27000 van del 27000 a 27019 i de 27030 a 27044 amb 27799 finalitzant la sèrie formalment en aquests moments.

En aquest apartat es pretén abordar el que recull cadascuna de les ISO quan s'han destacat en l'apartat anterior amb la finalitat de conèixer millor cadascuna de les ISO.

A continuació, es mostra, un esquema que representa l'evolució de la família 27000. Tal com podem veure en la il·lustració, les normatives relacionades amb l'evolució de la seguretat de la informació es remuten a la dècada del 1980, essent la normativa BS7799 la primera d'aquestes. Posteriorment, es pot veure l'evolució fins a data d'avui.



Il·lustració 04 - Història de la familia ISO 27000 i els seus estàndards. (PQBWeb, ISO 27000)

8.4.2.1. Normativa BS7799

En aquest primer apartat, descriurem la normativa BS7799 que fou creada a Gran Bretanya i que establia els estàndards per a la seguretat de la informació. Aquesta normativa va ser substituïda per la normativa ISO 27001, que proporciona un marc més complet i internacional per a la gestió de la seguretat de la informació.

La normativa BS7799 es va publicar per primera vegada en 1995 i es va actualitzar en 1999. Aquesta normativa, originalment, es dividia en dues parts:

D'una banda, la normativa BS7799-1: descrivia els requisits per a un sistema de gestió de la seguretat de la informació. En la pràctica, era una espècie de manual per a crear i gestionar un sistema de seguretat informàtica dins d'una organització.

D'altra banda, la normativa BS7799-2: se centrava en l'avaluació dels sistemes de gestió de la seguretat de la informació. En la pràctica, proporcionava els estàndards de referència per a avaluar la qualitat i eficàcia dels sistemes de seguretat informàtica.

Totes dues parts de la normativa BS7799 van ser posteriorment reemplaçades per la normativa ISO 27001, que es basa en els mateixos principis, però representa un estàndard més complet i actualitzat. La normativa ISO 27001 proporciona un marc complet per a la gestió de la seguretat de la informació, des de la planificació fins a l'avaluació i millora contínua.

8.4.2.2.ISO 27001-2013

Inicialment, fou publicada per primer cop el 15 d'octubre de 2005, revisada el 25 de setembre de 2013 (segona edició) i actualitzada el 25 d'octubre de 2022 (versió 3).L'ISO 27001:2013 es basa en l'enfocament de cicle de vida del SGSI, que inclou la planificació, implementació, revisió i millora contínua del sistema. Els requisits de la norma inclouen la identificació i gestió de riscos, la implementació de controls de seguretat, la gestió d'incidents i la millora contínua del SGSI.

8.4.2.3. ISO 27002-2021

La norma ISO 27002:2021, anteriorment coneguda com a ISO 27002:2013, és un codi de pràctiques per a la gestió de seguretat de la informació. Aquesta norma proporciona un conjunt complet de controls de seguretat de la informació que poden ser implementats per una organització per a millorar la seva postura de seguretat de la informació.

La norma ISO 27002:2021 estableix un marc per a la selecció, implementació, manteniment i millora dels controls de seguretat de la informació en una organització. La norma inclou un ampli conjunt de controls, organitzats en 14 seccions que cobreixen àrees com a polítiques de seguretat, gestió d'actius, control d'accés, gestió d'incidents, continuïtat del negoci, compliment legal i físic i seguretat ambiental.

8.4.2.4. ISO 27003:2017

La norma ISO 27003:2017 és una guia que proporciona una orientació detallada sobre com establir i mantenir un sistema de gestió de seguretat de la informació (SGSI) basat en la norma ISO 27001:2013.

Aquesta norma inclou informació sobre la planificació i el disseny del SGSI, la implementació i l'operació del sistema, l'avaluació i millora contínua del SGSI i la preparació per a la certificació del SGSI. La guia també inclou informació sobre la integració del SGSI amb altres sistemes de gestió i la gestió de riscos i oportunitats.

Cal destacar que la norma ISO 27003:2017 no és una norma certificable en si mateixa, sinó que proporciona una guia per a la implementació d'un SGSI basat en la norma ISO 27001:2013.

8.4.2.5. ISO 27004:2016

La norma ISO 27004:2016 és una guia que proporciona orientació sobre com mesurar l'efectivitat d'un Sistema de Gestió de Seguretat de la Informació (SGSI) i l'eficàcia dels controls de seguretat implementats en una organització.

La norma ISO 27004:2016 se centra en el mesurament i avaluació dels controls de seguretat de la informació i el SGSI en general. La guia estableix els requisits per al disseny i la implementació d'un programa de mesurament, incloent-hi els objectius, els indicadors de rendiment i les mesures d'efectivitat. També es proporciona informació sobre com analitzar i comunicar els resultats del mesurament. És important tenir en compte que la norma ISO 27004:2016 no és una norma certificable en si mateixa, sinó que proporciona orientació sobre el mesurament i avaluació dels controls de seguretat de la informació i el SGSI en general.

8.4.2.6. ISO 27005:2018

La norma ISO 27005:2018 és una guia que proporciona un marc de treball per a la gestió de riscos de seguretat de la informació en una organització. La norma es basa en la norma ISO/IEC 27001:2013 i proporciona una guia detallada sobre com implementar un procés de gestió de riscos efectiu.

La norma ISO 27005:2018 estableix els requisits i principis per a la gestió de riscos de seguretat de la informació, incloent-hi la identificació d'actius d'informació i les amenaces associades, l'avaluació de riscos i la selecció de mesures de seguretat adequades. També proporciona orientació sobre la implementació i operació del procés de gestió de riscos.

Cal tenir en compte que la norma ISO 27005:2018 no és una norma certificable en si mateixa, sinó que proporciona orientació sobre com implementar un procés de gestió de riscos de seguretat de la informació efectiu i eficient basat en la norma ISO/IEC 27001:2013.

8.4.2.7. ISO 27006:2015

La norma ISO 27006:2015 és una norma que estableix els requisits per a l'auditoria dels sistemes de gestió de seguretat de la informació (SGSI). La norma proporciona orientació sobre la competència i la imparcialitat dels auditors de SGSI, així com sobre els processos i procediments que s'han de respectar durant una auditoria.

La norma ISO 27006:2015 s'aplica a les organitzacions que busquen la certificació de la seva SGSI o que desitgen realitzar auditories internes o externes de la seva SGSI. La norma estableix els requisits que els auditors han de complir per a demostrar la seva

competència, imparcialitat i integritat. També estableix els requisits per al procés d'auditoria, incloent-hi la planificació, la realització de l'auditoria, la documentació i l'informe dels resultats.

Cal destacar que la norma ISO 27006:2015 no estableix els requisits per al SGSI en si mateix, sinó que estableix els requisits per a l'auditoria d'un SGSI.

8.5. Marc pràctic de la ISO, gestió integral

8.5.1. Primeres orientacions per a l’empresa

Quan una empresa es proposa aconseguir la certificació ISO esdevé una fita molt important que tindrà un impacte rellevant en l'organització de cara al futur. Obtenir la certificació ISO suposa un compromís per a implementar i mantenir sistemes de gestió eficaços en diversos aspectes de l’empresa.

A continuació, es detallen alguns dels aspectes més rellevants per tal d'assolir l'èxit en la certificació ISO:

- Suport de lideratge i gestió: Una certificació ISO requereix el lideratge i gestió per part de la direcció de l'organització. Aquesta ha de mostrar-se activa al llarg de tot el procés, dotant dels recursos necessaris així com promoure una cultura de millora contínua.

- Comprensió i aplicació de les normes ISO: les empreses han de comprendre a fons els requisits de la norma ISO per a la qual estan buscant la certificació, com l'ISO 27001 per a la gestió de la seguretat de la informació.

- Compromís i formació dels treballadors: més enllà de la capa executiva de l'empresa, els treballadors juguen un paper fonamental durant el procés de certificació ISO. Cal destacar, que s'han de dur terme diferents programes de formació per a poder assegurar que els empleats entenguin els requisits, les seves funcions i responsabilitats, i com contribuir eficaçment a la implementació i manteniment del sistema de gestió.

- Processos i procediments documentats: la certificació ISO requereix processos i procediments ben documentats que s'ajustin als requisits de l'estàndard. Aquests documents han de ser revisats i actualitzats regularment per reflectir els canvis en l'organització i millorar alguns aspectes com l'eficiència i l’eficàcia.

- Auditoria interna i revisions de gestió: les auditories internes regulars ajuden a identificar punts de millora.

- Accions correctives i preventives: Quan s'identifiquen desviacions, les empreses han de prendre les accions correctives i preventives adients per abordar les causes del problema i aconseguir revertir-lo. D'aquesta manera, es demostra un compromís ferm per mantenir la certificació ISO, així com, la millora contínua.

- Auditoria de certificació externa: per tal d'assolir la certificació ISO, cal que les empreses superin una auditoria de certificació externa realitzada a través d'un organisme acreditat. L'objectiu d'aquesta auditoria és verificar que el sistema de gestió de l'organització compleix els requisits de l'estàndard ISO. Si s'assoleixen tots els requisits establerts per l'estàndard, llavors s'adjudica la certificació ISO.

- Manteniment i millora constant: la certificació ISO no és una fita única. Les empreses han de mantenir i millorar constantment els seus sistemes de gestió per garantir el compliment continu de l'estàndard ISO.

Un cop descrits els factors clau, convé destacar que si aquests han estat implementats, llavors qualsevol empresa augmentarà d'una forma significativa les seves possibilitats d'aconseguir i mantenir amb èxit la certificació ISO. Les organitzacions han de mantenir el seu compromís amb la millora contínua per recollir tots els beneficis de la certificació.

A més a més, està demostrat que les empreses que assoleixen una certificació ISO experimenten avantatges directament relacionats amb el rendiment de la inversió (ROI), una millor eficiència de l'empresa que permet reduir les despeses i fins i tot augmentar el nombre de clients donat el prestigi i reconeixement en l'àmbit empresarial que suposa haver superat una certificació ISO.

8.5.2. Aspectes clau per a la selecció d'una empresa Consultora

La guia pretén recollir la informació més rellevant i servir com un suport, tot i això, es recomana que per tal de dur a terme la implementació de qualsevol normativa ISO i la seva posterior certificació, es faci mitjançant empreses de consultoria certificades. Aquestes empreses compten amb professionals altament qualificats que ens acompanyaran al llarg de tot el procés i ens assessorin a prendre les millors decisions de cara a la nostra organització.

Alguns dels aspectes més importants per tal de seleccionar una empresa de consultoria són:

- Sol·licitar referències en casos d'èxits previs.

Conèixer altres casos d'èxit que ha dut a terme l'empresa consultora ens ajudarà a veure com treballen.

- Quina és l'empresa consultora més adequada per a la nostra empresa?

És fonamental que la manera de treballar i estil de l'empresa que ofereix els serveis de consultoria siguin comuns i es creï una bona relació per tal de contribuir a una associació exitosa.

- Ofereixen serveis addicionals?

Cal valorar l'opció de contractar serveis addicionals que ens ajudaran a fer la correcta implementació.

- Ofereixen flexibilitat? S'adaptaran a les nostres necessitats?

Cal destacar que és molt important que l'empresa consultora ens ajudi en el procés de certificació, però també inclogui un pla de formació.

- La planificació temporal.

Cal escollir una empresa de consultoria que sigui realista amb el procés d'implementació. Per assolir l'èxit caldrà que el consultor conegui de primera mà el funcionament de la nostra empresa.

- I després de la certificació ISO?

El màrqueting jugarà un paper molt rellevant. Una certificació ISO ha d'esdevenir un fet del qual l'empresa ha de promoure entre els seus clients i col·laboradors.

Aquestes són algunes de les consideracions per tal de poder escollir la millor consultora que s'ajusti a les nostres necessitats. És evident, que caldrà estudiar diferents propostes

per poder escollir correctament i que la certificació ISO en la nostra empresa esdevingui un cas d'èxit.

8.5.3. Aplicació de la normativa

Tal com ja és s'ha descrit prèviament, la norma ISO 27000 té un conjunt de normes que en formen part. Ara bé, en aquest apartat donarem una visió pràctica de la família ISO 27000 i en detallarem, segons la seva importància i criticitat quines de les normatives són recomanables per a començar a implementar. És evident, que en una petita o mitjana empresa, no es pot fer un desplegament de totes les normatives de forma directa sinó que caldrà estudiar cada cas concret i definir un full de ruta.

8.5.3.1.La norma ISO 27000 i el conjunt d'estàndards de Seguretat de la Informació

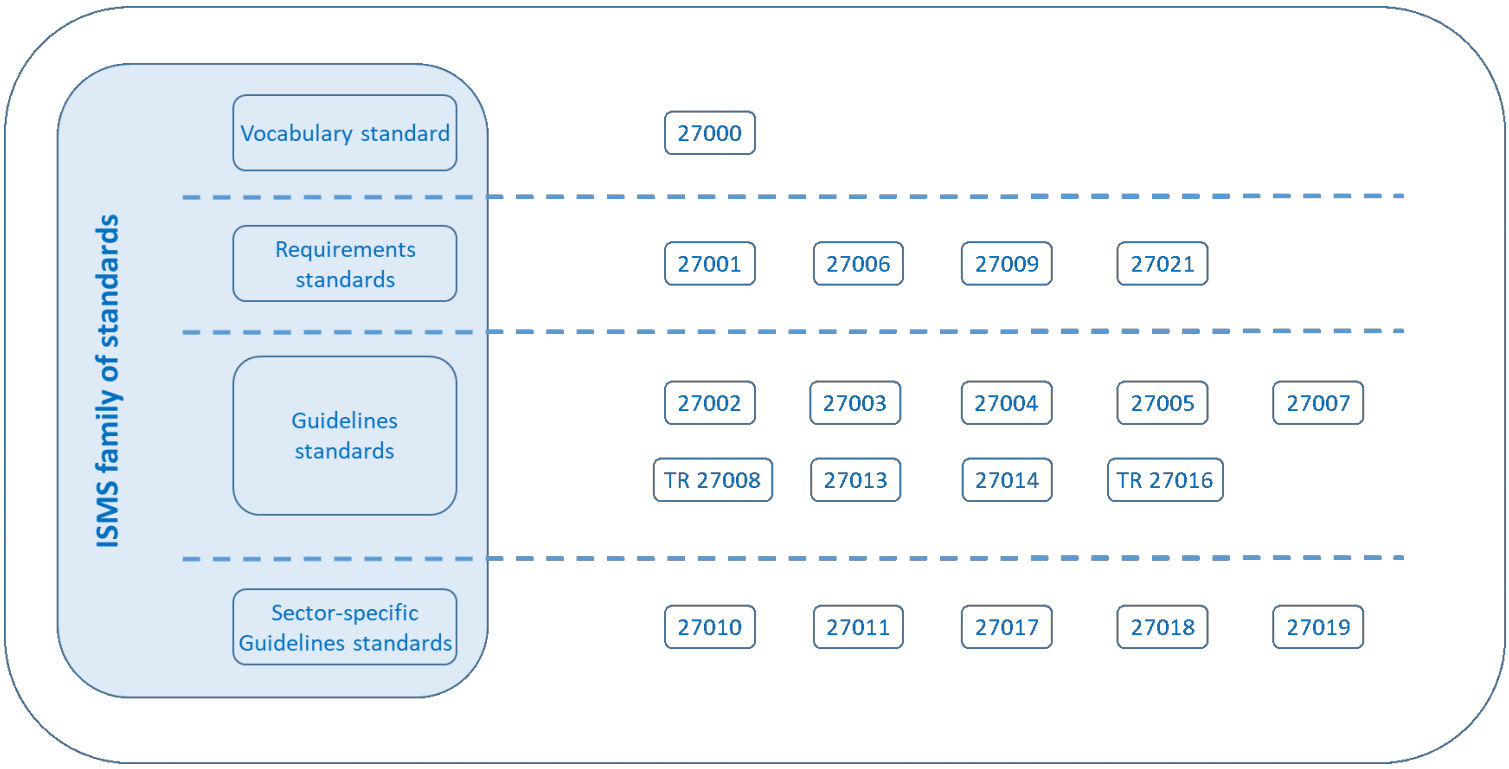
En aquest apartat es vol donar una visió pràctica de la norma ISO 27000 i, de forma breu, fer un repàs descriptiu de quines són les diferents normes que engloben dita norma.

- Què és la norma ISO 27000?

L'ISO 27000 és una sèrie de normes internacionals desenvolupades i gestionades per l'Organització Internacional per a l'Estandardització (ISO) i la Comissió Electrònica Internacional (IEC). Aquestes normes proporcionen directrius i bones pràctiques per a l'establiment, implementació i gestió d'un Sistema de Gestió de Seguretat de la Informació (SGSI) o Information Security Management System (ISMS). La sèrie ISO 27000 permet establir les bases i aporta un llenguatge comú per a la resta de les normes de la sèrie.

Aquesta sèrie engloba diverses normes específiques, com l'ISO 27001, que estableix els requisits per a la implementació i gestió d'un SGSI certificable. A més a més, també existeix l'ISO 27002, que defineix un conjunt de 114 controls agrupats en 14 dominis per a la implementació del SGSI.

Per tal d'implementar la normativa ISO 27000 i assolir la certificació necessària cal establir les diferents normes que caldrà tenir en compte de la sèrie. A continuació, es mostra una il·lustració que recull les diferents normatives que formen part de la família.



Il·lustració 05 - Família d'estàndards ISO 27000. (International Electrotechnical Commission)

- Quines són la resta de normes de la sèrie ISO 27000?

  - ISO 27001: Estableix els requisits necessaris per a implementar i gestionar un Sistema de Gestió de Seguretat de la Informació (SGSI). La norma ISO 27001 es pot certificar.

  - ISO 27002: Defineix un conjunt de millors pràctiques per a la implementació del SGSI, a través de cent catorze controls organitzats en catorze dominis i trenta-cinc objectius de control.

  - ISO 27003: Facilita una guia per a la correcta implementació d'un SGSI, centrant-se en els aspectes clau per a aconseguir una implementació satisfactòria.

- ISO 27004: Ofereix pautes per a definir i establir mètriques que permeten avaluar adequadament el rendiment del SGSI.

- ISO 27005: Estableix les definicions sobre com gestionar els riscos relacionats amb els sistemes de gestió de la informació, incloent-hi la metodologia a utilitzar.

- ISO 27006: Estableix els requisits que han de complir les organitzacions que desitgin ser acreditades per a certificar el compliment de l'ISO/IEC 27001 a altres organitzacions.

- ISO 27007: Proporciona procediments per a realitzar auditories internes o externes amb la finalitat de verificar i certificar la implementació de l'ISO/IEC 27001.

- ISO 27008: Defineix com avaluar els diferents controls del SGSI per a revisar la seva adequació tècnica i la seva eficàcia en la correcta mitigació de riscos.

- ISO 27009: Complementa la norma ISO 27001. Aquesta inclou diferents requisits i controls addicionals aplicables a sectors específics, amb l'objectiu de millorar la seva implementació.

- ISO 27010: Indica com ha de tractar-se la informació compartida entre organitzacions, identificant riscos i els controls necessaris per a mitigar-los, especialment en infraestructures crítiques.

- ISO 27011: Estableix principis per a implementar, mantenir i gestionar un SGSI en organitzacions de telecomunicacions. També inclou pautes per a la implementació eficient dels controls.

- ISO 27013: Ofereix una guia per a integrar les normes ISO 27001 (SGSI) i ISO 20000 (Sistema de Gestió de Serveis - SGS) en organitzacions que implementen ambdues.

- ISO 27014: Estableix principis per al govern de la seguretat de la informació, permetent a les organitzacions avaluar, recopilar i comunicar les activitats relacionades amb la seguretat de la informació.

- ISO 27015: Facilita els principis d'implementació d'un SGSI a les empreses que ofereixen serveis financers.

- ISO 27016: Proporciona una guia per a la presa de decisions econòmiques relacionades amb la gestió de la seguretat de la informació. Aquesta guia serveix com a suport a les direcció de les organitzacions.

- ISO 27017: Ofereix una guia de 37 controls específics per a serveis en el núvol, basats en la norma ISO 27002.

- ISO 27018: Complementa les normes ISO 27001 i ISO 27002 en la implementació de procediments i controls per a protegir dades personals en organitzacions que ofereixen serveis en el núvol a tercers.

- ISO 27019: Proporciona una guia basada en la norma ISO 27002 per a aplicar en indústries relacionades amb el sector energètic, permetent la implementació d'un SGSI.

8.5.4. Aplicació de la normativa d'acord amb la importància i criticitat per a les petites i mitjanes empreses

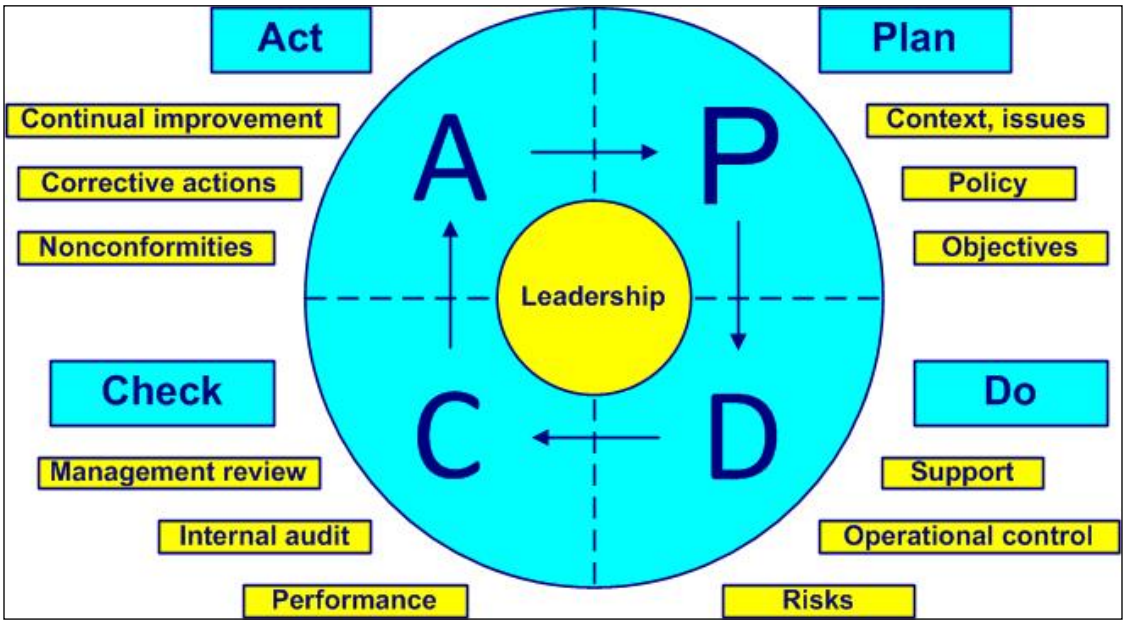
En l'entorn empresarial actual, la seguretat de la informació s'ha convertit en un aspecte crític per a l'èxit i la supervivència de les organitzacions. Les petites i mitjanes empreses (Pimes) no són l'excepció, ja que també enfronten amenaces cibernètiques cada vegada més sofisticades i riscos associats a la protecció de les dades i la confidencialitat de la informació.

En aquest context, l'aplicació de les normatives ISO 27001 i 27002 es torna essencial per a garantir una gestió eficaç de la seguretat de la informació.

D'una banda, l'ISO 27001 de vital importància atès que s'especifiquen els requisits necessaris per a implantar, mantenir i gestionar un SGSI. Habitualment, un cop implantada cal continuar mantenint i gestionant el nostre propi SGSI per continuar donant el compliment adequat a la normativa. És llavors, quan és clau disposar del que es coneix com a cicle PDCA o Cicle de Deming.

El cicle PDCA és una metodologia de gestió que té com a principal objectiu contribuir a la millora constant dels processos. Aquest cicle, tal com podem veure en la il·lustració, es basa en quatre passos diferents: *Plan, Do, Check & Act* (PDCA).

A continuació, es mostra una il·lustració que mostra de manera gràfica en què es basa el cicle de Deming. Convé destacar que en cadascun dels quatre passos (PDCA), existeixen alguns aspectes claus que estan directament relacionats amb cada pas específic.



Il·lustració 06 - El cicle de Deming. (PQBWeb, The Deming cycle)

D'altra banda, la 27002, és un conjunt de 114 controls, agrupats en 14 dominis diferents, que tenen com a objectiu dotar de bones pràctiques en relació amb la gestió del SGSI.

8.5.4.1. Consideracions en relació amb l'ISO 27001

L'aplicació de la normativa ISO 27001 és important, ja que estableix els requisits per al disseny, implementació, manteniment i millora contínua d'un Sistema de Gestió de Seguretat de la Informació (SGSI).

Per a les Pimes, adoptar aquesta normativa implica diferents beneficis significatius, com per exemple:

- Protecció de la informació confidencial: L'ISO 27001 proporciona un marc integral per a identificar i gestionar els riscos de seguretat de la informació, la qual cosa permet a les

Pimes protegir els seus actius més valuosos, com la propietat intel·lectual, les dades dels clients i la reputació de l'empresa.

- Compliment normatiu: L'adopció de la norma ISO 27001 ajuda a les Pimes a complir amb els requisits legals i reguladors relacionats amb la seguretat de la informació. Això és especialment rellevant en sectors altament regulats, com la salut, les finances i el comerç digital.

- Avantatge competitiu: Obtenir la certificació ISO 27001 pot ser un diferenciador clau per a les Pimes, ja que demostra el seu compromís amb la seguretat de la informació i genera confiança en els clients i socis comercials.

8.5.4.2. Consideracions en relació amb l'ISO 27002

La norma ISO 27002 esdevé també clau, donada la seva criticitat, atès que aquesta proporciona directrius i bones pràctiques per a la implementació de controls de seguretat de la informació. Encara que no és certificable per si mateixa, és complementària a la norma ISO 27001 i juga un paper crític en la gestió efectiva de la seguretat de la informació en les Pimes.

Alguns aspectes rellevants a considerar són:

- Selecció de controls adequats: La norma ISO 27002 proporciona un catàleg de controls de seguretat que es poden adaptar a les necessitats i recursos de les Pimes. Això permet a les empreses seleccionar els controls més rellevants i efectius per al seu entorn operatiu.

- Protecció integral: L'ISO 27002 abasta diversos aspectes de seguretat de la informació, com la gestió d'accessos, la seguretat dels actius, la seguretat física i ambiental, la gestió d'incidents, entre altres. Quan s'implementen aquests tipus de controls, les Pimes poden mitigar els riscos i assegurar una protecció integral de la seva informació.

- Enfocament basat en el risc: La norma ISO 27002 promou un enfocament de gestió de la seguretat de la informació basat en l'anàlisi de riscos. D'aquesta manera, les Pimes poden identificar i prioritzar els riscos rellevants, assignar els recursos més adients i establir mesures de mitigació eficients.

8.5.5. El paper clau de l'ISO 27001 i 27002 en les PIME

L'adopció de les normatives ISO 27001 i 27002 no únicament ho podem considerar com una mesura de seguretat, sinó també com una estratègia per a garantir la sostenibilitat i l'èxit en el futur de les PIME. Aquestes dues normatives permeten a les PIME dotar de protecció la seva reputació i evitar les conseqüències negatives dels incidents de seguretat que poden acabar desencadenant la pèrdua de clients, multes per infraccions comeses o, fins i tot, danys en la imatge de l'empresa.

Les dues normatives permeten a les PIME protegir la seva informació, complir amb els requisits normatius establerts i obtenir un avantatge competitiu en un entorn empresarial cada vegada més digitalitzat. És fonamental que les PIME puguin reconèixer la importància d'aquestes normatives i les incorporin en la seva estratègia de seguretat de la informació per a garantir el seu èxit. Per un costat, la norma ISO 27001 proporciona un marc robust per a la gestió de la seguretat de la informació, mentre per l'altre, la norma ISO 27002 ofereix directrius pràctiques per a la implementació de controls de seguretat efectius.

En resum, l'aplicació de les normatives ISO 27001 i 27002 és essencial perquè les PIME puguin enfrontar els desafiaments en el futur pròxim. En adoptar un enfocament proactiu i enfocat en el risc, les PIME poden protegir els seus actius més valuosos. La seguretat de la informació no ha de ser menyspreada, i les PIME que posin aquest punt com una prioritat en la seva estratègia empresarial estaran més ben posicionades per a aconseguir l'èxit a llarg termini en un món digitalitzat i en constant evolució.

8.5.6. Estructura de la norma ISO 27001

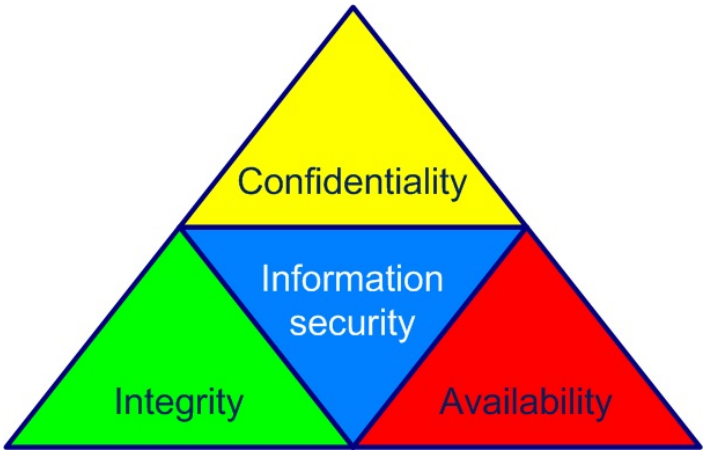
La Norma ISO 27001 estableix els requisits per a implementar un Sistema de Gestió de la Seguretat de la Informació (SGSI). Aquest sistema s'enfoca a adoptar mesures per a protegir la informació en qualsevol format contra diverses amenaces, assegurant la continuïtat de l'empresa.

Els objectius principals del SGSI són tres:

1. Confidencialitat: Garantir que la informació només sigui accessible per les persones autoritzades i es mantingui protegida enfront d'accessos no permesos.

2. Integritat: Cal assegurar que la informació sigui precisa, completa i estigui protegida contra modificacions no autoritzades o manipulacions indegudes, garantint la seva exactitud.

3. Disponibilitat: Mantenir la informació disponible i accessible quan es requereixi, assegurant la seva disponibilitat per a les persones autoritzades i evitant interrupcions o denegacions del servei. Aquests objectius busquen salvaguardar la informació de l'organització, assegurant la seva confidencialitat, integritat i disponibilitat en tot moment.



Il·lustració 07 - Les principals propietats de la seguretat de la informació. (PQBWeb, Information security properties)

Tal com podem veure en la il·lustració anterior, els objectius detallats anteriorment busquen salvaguardar la informació de l'organització, assegurant la seva confidencialitat, integritat i disponibilitat en tot moment.

8.5.6.1. Fases per a la implementació d'un SGSI

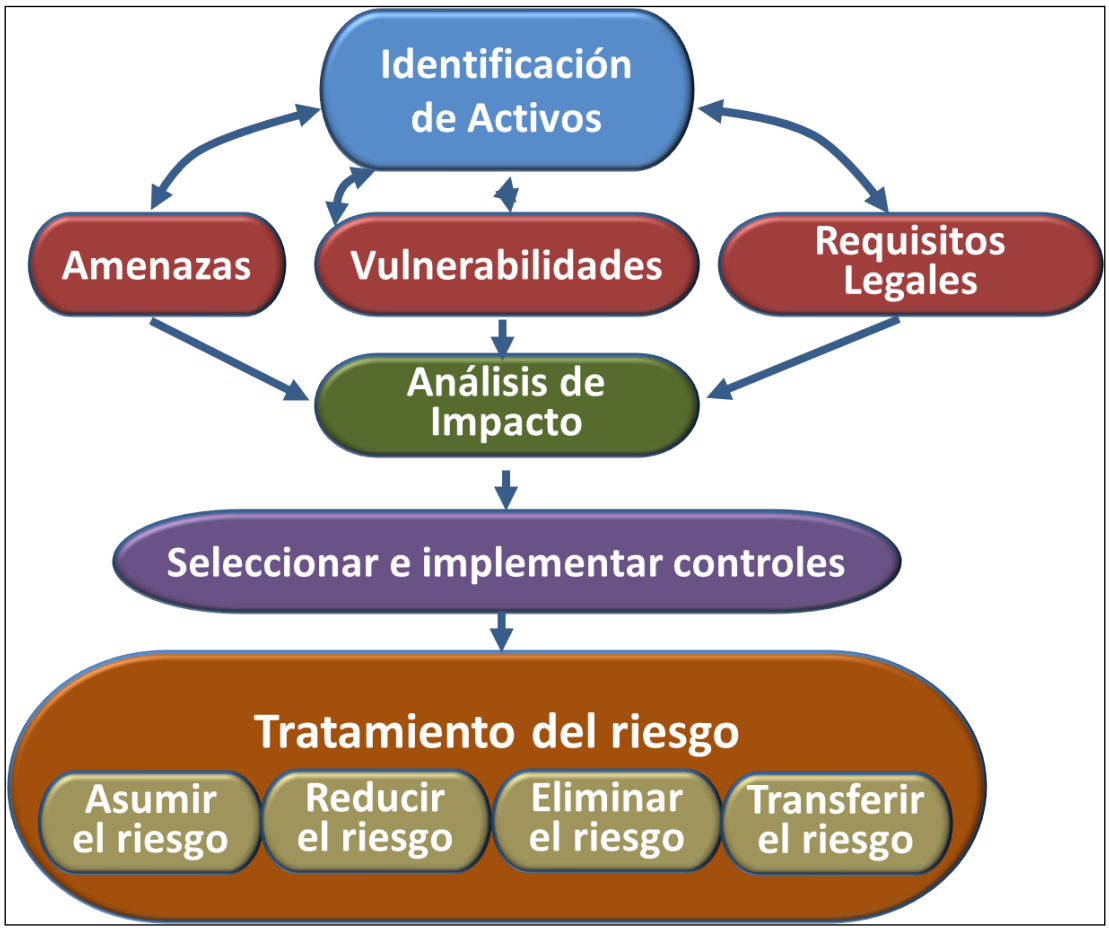
Per tal de dur a terme la correcta implementació del SGSI d'acord amb la normativa 27001 caldrà seguir les fases que es mostren en la figura que trobem a continuació. Tal com podem veure en la il·lustració, es tracta d'un conjunt de set fases diferents.

Il·lustració 08 - Principals fases per a la implementació d'un SGSI. (Normas-ISO, SGSI)

8.5.6.2. L'avaluació de Riscos

L'element central per a dur a terme la correcta en la implementació d'un Sistema de Gestió de la Seguretat de la Informació (SGSI) basat en la norma IS0 27001 és clau enfocar-ho mitjançant l'Avaluació de Riscos.

En concret, aquest aspecte de la norma dona a la part executiva de l'organització una visió integral per a poder definir d'una forma clara i concisa l'abast i aplicació del SGSI. D'aquesta manera, també, s'aconsegueix establir un enfocament coherent i sistemàtic per donar continuïtat a la integració de la normativa en el futur. En primer lloc, convé escollir una metodologia d'avaluació de riscos adequada als requisits del negoci. Existeixen diverses metodologies estandarditzades disponibles per a dur a terme aquesta tasca. A continuació, es prendrà com a punt de partida la metodologia suggerida en la norma.



Il·lustració 09 - Metodologia per a l'avaluació i tractament dels riscs. (Normas-ISO, Evaluación de Riesgos)

A continuació, descriurem el mètode a seguir per a l'avaluació i tractament dels riscos. Aquest mètode està estructurat en set punts diferents els quals són:

1. Identificació dels actius d'informació i els seus responsables: Consisteix a identificar tots els elements que tenen valor per a l'organització. Cal incloure tots els elements que tenen valor per a l'empresa ja siguin a escala física, intel·lectual, així com la marca i la reputació. Cada actiu ha de tenir un responsable designat.

2. Identificació de les vulnerabilitats: Es tracta d'identificar les febleses inherents a cada actiu que el fan susceptible a sofrir alguna mena d'atac o dany perjudicial.

3. Identificació d'amenaces: Consisteix a identificar les situacions que podrien causar danys als actius d'informació, com per exemple: els incendis o l'espionatge, entre altres.

4. Identificació de requisits legals i contractuals: És necessari identificar els requisits establerts per la legislació i els contractes que l'organització ha de complir amb relació als seus clients, socis o proveïdors.

5. Identificació de riscos: En aquest pas es determina la probabilitat que les amenaces o les vulnerabilitats de cada actiu puguin ocasionar danys parcials o totals en termes de disponibilitat, confidencialitat i integritat de la informació.

6. Càlcul del risc: Es realitza un càlcul del risc considerant la probabilitat d'ocurrència i l'impacte que podria tenir en l'organització. D'aquesta manera, s'aconsegueix dona prioritat als riscos que requereixen major atenció.

7. Pla de tractament del risc: En aquesta etapa es defineix la política de tractament dels riscos, tenint en compte els passos anteriors i la direcció estratègica de l'organització. Cal seleccionar els controls adequats per a cada risc, amb l'objectiu d'assumir, reduir, eliminar o transferir el risc identificat.

8.5.7. Estructura de la norma ISO 27002

Primerament, cal destacar que la norma ISO 27002 a diferència de la norma 27001, no és certificable. És a dir, l'ISO 27002 el podem definir com un estàndard que dona suport i és complementari a la normativa ISO 27001. L'ISO 27001 és certificable atès que defineix el sistema de gestió de la seguretat de la informació (SGSI).

En relació amb l'ISO 27002 cal destacar que disposa d'una versió força recent, en concret, dita normativa fou creada l'any 2005 i actualitzada per últim cop l'any 2022.

A continuació, es presenta un esquema amb l'objectiu de clarificar i ajudar a comprendre quins canvis ha sofert la normativa ISO 27002 de l'any 2013 vers l'última versió publicada l'any 2022.

Il·lustració 10 - Novetats en la Norma ISO 27002 (AENOR, Las referencias en ciberseguridad se actualizan)

Aquesta normativa està estructurada de la següent manera:

- Introducció: En aquesta secció, es posa en relleu el context del valor de la informació per a les organitzacions i com s'aconsegueix la seguretat de la informació mitjançant la implementació d'un conjunt de controls de seguretat. S'expliquen els requisits necessaris de seguretat de la informació que una organització ha d'establir, així com la selecció de diferents controls per a protegir-la. D'altra banda, també es considera el cicle de vida de la informació, és a dir, des de la seva creació fins a la seva destrucció. Finalment, s'analitza la relació de la norma ISO 27002 amb la resta de normatives de la família ISO 27000.

- Clàusula 1 - Abast: Aquest document es presenta com una guia de referència per a les organitzacions on el seu objectiu és proporcionar orientació i suport en el procés de selecció dels controls adequats per a garantir la seguretat de la informació de l'organització.

- Clàusula 2 - Referències normatives: la norma ISO 27002 no conté referències normatives.

- Clàusula 3- Termes, definicions i abreviatures: d'acord amb el context de la normativa, es presenten diversos termes i definicions.

- Clàusula 4 - Estructura del document: es detalla les clàusules, els temes i l'estructura de cada control.

- Clàusules de la 5 a la 8: s'estableix informació relacionada amb el propòsit o una guia d'implementació pel que fa als controls de seguretat. Aquests controls de seguretat estan separats en diversos àmbits els quals són:

    - Clàusula 5: en l'àmbit organitzacional
    - Clàusula 6: en l'àmbit de les persones
    - Clàusula 7: en l'àmbit físic
    - Clàusula 8: en l'àmbit tecnològic

- Annex A: s'exposa una taula per a ajudar a comprendre l'ús dels atributs per tal de crear diferents punts de vista pel que fa als controls de seguretat.

- Annex B: s'exposa la correspondència entre les dues últimes versions de l'ISO 27002.

- Bibliografia: es mostra la relació amb la resta de normes.

8.5.8. Preguntes freqüents

Les preguntes freqüents és l'apartat final de la guia dissenyat exclusivament a donar una resposta clara i senzilla a les preguntes que sovint una empresa es pot plantejar en relació amb el procés d'implementació de les normatives ISO.

- Com es creen les normatives ISO?

El comitè tècnic compost per delegats nacionals experts duu a terme diferents debats, amb l'objectiu d'elaborar un esborrany. Posteriorment, es reuneixen els membres de l'ISO per a revisar i sotmetre a una votació l'esborrany. Si la votació dona un resultat favorable, el document es publica com una Norma Internacional. En cas contrari, la norma és sotmesa a una segona revisió. Posteriorment, es realitza una nova redacció i es repeteix el procés de votació.

- Qui crea les normes ISO?

Les normes ISO són creades per comitès tècnics internacionals conformats per experts de diferents àmbits industrials. Cada any, una gran quantitat de persones altament qualificades, incloent-hi representants governamentals i associacions de consumidors, participen activament en el procés de desenvolupament de les normatives ISO.

- Quin significat té la ‘Normalització Internacional’?

La normalització internacional ofereix un marc de referència o un llenguatge tecnològic compartit entre proveïdors i clients, la qual cosa facilita el comerç i la transferència de tecnologia. El principal objectiu de la normalització és aconseguir establir un estàndard comú en tot un sector empresarial en concret.

- Es mantenen actualitzades les normes ISO?

Les normes ISO són sotmeses a revisions de forma periòdica. S'estableix un període mínim de revisió cada cinc anys des de la seva publicació. Per tal de garantir la seva validesa contínua la normativa se sotmet a un procés de revisió, anàlisi i actualització.

- Quins factors són clau per obtenir les normes ISO? Quant temps triga a completar-se tot el procés?

El procés per a completar la certificació d'una normativa ISO depèn de diversos factors clau. Alguns dels factors més rellevants són el nombre de seus, els empleats de l'empresa o les normatives a implementar. Per tant, caldrà que una empresa especialitzada ens orienti en el temps estimat en funció de cada empresa i les necessitats que aquesta tingui.

- És molt elevat el cost d'implementar la normativa ISO?

El cost de la implementació de la normativa ISO depèn de diversos factors com poden ser la grandària de l'empresa, les normatives ISO a implementar, el nombre d'empleats i les possibles adaptacions o modificacions a fer en l'organització en estudi per tal de garantir que se satisfan tots els requisits establerts per l'ISO a certificar. Per tant, caldrà en cada cas fer un estudi per a poder disposar d'un càlcul adequat.

- Les petites i mitjanes empreses poden assumir aquest cost?

Existeixen diferents empreses del sector que ofereixen assessorament especialitzat per a petites i mitjanes empreses. Cal destacar que és habitual que les empreses puguin aconseguir finançament amb condicions interessants.

9. Conclusions

Un cop feta la recerca i finalitzada la redacció de la memòria escrita, és moment, d'analitzar els resultats obtinguts tot comparant-los amb els objectius inicials.

A parer meu, aquests objectius han estat extensament investigats i m'han permès assolir un alt grau de coneixement sobre el món teòric i pràctic del de les normatives ISO, especialment, l'ISO 27001 i 27002.

Altrament, els objectius no han constituït un element independent dintre del Treball de Fi de Grau sinó que han format una part molt important de l'elaboració del treball.
Convé ressaltar que aquests han estat el punt de partida per organitzar i conduir la memòria.

El primer objectiu tenia com a finalitat conèixer de manera detallada a escala teòrica i tècnica les diferents normatives ISO que envolten el món de la ciberseguretat.Aquest s'explica vastament al llarg de la primera part de la guia i m'ha servit per poder relacionar-lo amb la part més pràctica, és a dir, els apartats dedicats a les normatives ISO 27001 i ISO 27002.

El segon objectiu perseguia investigar principalment l'ús de les normatives ISO en diversos àmbits i valorar els seus pros i contres. Aquest procés de recerca m'ha facilitat projectar i aplicar els coneixements assolits, lligar-los amb el món empresarial i presentar la posterior guia.

Amb el darrer objectiu es pretenia presentar una guia amb les orientacions necessàries perquè una pime pugui iniciar el procés d'implementació i, si escau, el de certificació d'una normativa ISO. En concret, s'ha abordat l'ISO 27001 i l'ISO 27002. Cal destacar que la primera d'aquestes és una normativa certificable mentre que l'altra no ho és. Facilitar el procés d'una empresa a emprendre el camí d'implementar la normativa ISO i alhora millorar el seu rendiment empresarial.

Avui en dia, el nombre de ciberatacs és una xifra a l'alça on les empreses, i la societat en general, ens enfrontem enfronta a retallades pressupostàries, pocs recursos, i demandes creixents per part de la societat. La ciberseguretat s'ha introduït a les empreses però no sempre en les millors condicions. Un exemple concret, el trobem en les pimes. Les quals

fer front a una implementació i certificació d'una normativa ISO els suposa un gran esforç a escala econòmica però també pel que fa als recursos temporals.

Fer el salt i apostar per l'assessorament d'una empresa especialitzada en la implementació de les normatives ISO, és una evolució que no només aporta millores tecnològiques a l'empresa sinó també millores en l'àmbit empresarial. Assolir una certificació suposa que l'organització es trobi més ben preparada per fer front als reptes en matèria de ciberseguretat i alhora posicionar-se en el mercat com una empresa capdavantera i adaptada a les necessitats del món actual. També, suposaria una nova manera d'organitzar i protegir tota la informació relacionada amb l'organització.

Després de la recerca i la presentació de la guia puc afirmar que la implementació de l'ISO 27001 i 27002 pot aportar molts avantatges a qualsevol pime però amb matisos. És possible que inicialment començar el procés d'implementació no resulti avantatjós econòmicament, ja que cal fer una despesa elevada. Perquè aquesta implementació pogués resultar atractiva en l'àmbit econòmic, seria necessària un ferm compromís per part de l'empresa així com estudiar-ne la viabilitat empresarial en el futur.

Deixant de banda el nivell econòmic penso que especialment, la implementació de la normativa ISO 27001, suposaria bàsicament la millora en la gestió de la informació. Convé destacar que una gran part de la informació de qualsevol organització es troba en els sistemes informàtics; tot i això, la normativa ISO 27001 va més enllà, incloent-hi el coneixement de les persones que integren la companyia, que també esdevé informació. Per tant, aquesta normativa proposa un marc de gestió integral de la seguretat de la informació de qualsevol organització.

És a dir, convé posar èmfasi en els sistemes informàtics, però també caldrà gestionar la informació concebuda com el coneixement, entre altres, per tal de protegir integralment tota la informació que pertany a l'empresa.

La guia presentada ha de ser concebuda com una guia preparada per a ser adaptada i millorada d'acord amb les necessitats canviants de les empreses. Per tant, podria recomanar-se com una prova pilot a seguir per a petites o mitjanes empreses que volguessin establir un sistema de gestió de la seguretat de la informació (SGSI).

Analitzats els objectius i redactades les conclusions, en aquests moments de la memòria, dono per acabat el meu treball d'investigació exposat al llarg de les pàgines anteriors. Personalment, valoro positivament la tasca duta a terme iconsidero superades les inquietuds, temors i entrebancs que han sorgit al llarg del Treball de Fi de Grau.

Una vegada més, vull mostrar el meu agraïment a totes les persones que l'han fet possible.

10. Glossari

- Actiu: Qualsevol element com per exemple edificis, persones, sistemes o informació que sigui considerada d'alt valor per a l'organització.

- Amenaça: Indici rellevant que pot desencadenar en un incident no desitjat. Els efectes poden provocar danys greus per a l'organització.

- Avaluació de riscos: Procés al qual és sotmès qualsevol risc per a determinar-ne la naturalesa així com la perillositat d'aquest.

- Autenticació (MFA): Mètode de control d'accés per tal de confirmar l'autenticitat d'un usuari després que aquest presenti dues o més proves per tal de garantir que és qui diu ser.

- Ciberespai: Espai virtual en què els cibernautes, habitualment mitjançant internet, interactuen amb altres usuaris i duen a terme les seves activitats.

- Ciberincident: Qualsevol succés que pugui desencadenar un risc per a la seguretat de les xarxes i sistemes d'informació d'un usuari o organització.

- Ciberseguretat: En informàtica, l'acció de protegir els sistemes, xarxes i dades vers les amenaces d'un ciberatac o d'altres ciberincidents generalment mitjançant internet.

- Confidencialitat: Propietat de la informació de no ser revelada o posar-se a disposició de tercers sense un consentiment explícit.

- Control: Totes les accions destinades a mantenir els riscos de seguretat de la informació per sota del nivell de risc prèviament establert.

- Disponibilitat: Propietat de la informació de mantenir la informació disponible i accessible quan es requereixi per part d'un tercer degudament autoritzat.

- DDoS: De les seves sigles en anglès (*Distributed Denial-of-Service Attack*), en termes de seguretat informàtica, és un atac a un sistema o xarxa que causa que un servei o recurs sigui inaccessible als usuaris legítims.

- IA (Intel·ligència Artificial): Combinació d'algorismes dissenyats amb l'objectiu de crear màquines que presentin capacitats similars a les de l'ésser humà.

- IDS: De les seves sigles en anglès (Intrusion Detection System), és un sistema de seguiment que detecta activitats sospitoses i genera alertes quan es detecten.

- Impacte: El cost, no únicament en termes econòmics, que suposa per a qualsevol organització patir un incident.

- Incident: En termes de seguretat de la informació, esdeveniment o conjunt d'esdeveniments de seguretat nodesitjats que generen una probabilitat rellevant d'amenaçar la seguretat de la informació i posar en risc la continuïtat del negoci.

- IoT: De les seves sigles en anglès (The Internet of Things), descriu els objectes físics incrustats amb sensors que es comuniquen amb els sistemes informàtics a través de la xarxa sense fils.

- ISO 27000: Conjunt d'estàndards internacionals sobre la Seguretat de la Informació.

- ISO 27001: Especificacions necessàries per a la implementació d'un Sistema de Gestió de laSeguretat de la Informació (SGSI).

- ISO 27002: Codi que recull un seguit de bones pràctiques que fan referència a la gestió de la seguretat de la informació.

- Integritat: Propietat de la informació per tal de garantir que aquesta sigui exacta i precisa.

- Machine Learning: Branca de la informàtica que es basa en l'ús d'algorismes i dades per tal de recrear la forma com els humans aprenen.

- Malware: En termes de seguretat informàtica programari maliciós.

- Milestone: Objectiu a assolir en el desenvolupament d'una tasca.

- PDCA (Plan-Do-Check-Act): Conegut com el cicle de Deming, és una metodologia per millorar la qualitat de forma ininterrompuda.

- Phising: Enviament de correus maliciosos dissenyats per enganyar els seus destinataris amb l'objectiu d'aconseguir que els usuaris revelin dades confidencials.

- SGSI: Sistema de gestió de la seguretat de la informació, són el conjunt d'elements que fa servir una organització per a definir una política i uns objectius de seguretat de la informació.

- Spear phishing: Tipus de phishing que s'adreça a una persona o grup amb informació d'interès per al destinatari, com documents financers.

- Tallafoc: En informàtica, programa d'un servidor d'accés a una xarxa local que s'encarrega de la gestió i control de les comunicacions amb xarxes externes per tal de garantir-ne la seguretat.

- Vulnerabilitat: Feblesa d'un control o actiu que pot ser explotada mitjançant qualsevol mena d'amenaça.

11. Bibliografia

- *INCIBE* [en línia] [consulta: 6 de març de 2023]. Disponible a: https://www.incibe.es/empresas/blog/tienes-hoja-ruta-ciberseguridad-tu-empresa
- *Astra* [en línia] [consulta: 8 de març de 2023]. Disponible a: https://www.getastra.com/blog/security-audit/cyber-security-statistics/
- *UNE* [en línia] [consulta: 8 de març de 2023]. Disponible a: https://www.une.org/
- *INCIBE* [en línia] [consulta: 12 de març de 2023]. Disponible a: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
- *ISO.org* [en línia] [consulta: 16 de març de 2023]. Disponible a: https://www.iso.org/obp/ui/#home
- *ISO.org* [en línia] [consulta: 18 de març de 2023]. Disponible a: https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:es
- *ISO.org* [en línia] [consulta: 18 de març de 2023]. Disponible a: https://www.iso.org/obp/ui#iso:std:iso:26000:ed-1:v1:es
- *ISO.org* [en línia] [consulta: 18 de març de 2023]. Disponible a: https://www.iso.org/obp/ui#iso:std:iso:37001:ed-1:v1:es
- *IEC* [en línia] [consulta: 25 de març de 2023]. Disponible a: https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iso-27000-series/
- *The Hack Notes* [en línia] [consulta: 26 d'abril de 2023]. Disponible a: https://blog.thehacknotes.com/p/norma-iso-27001-27002/
- *GlobalSuite Solutions* [en línia] [consulta: 26 d'abril de 2023]. Disponible a: https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/
- *GlobalSuite Solutions* [en línia] [consulta: 26 d'abril de 2023]. Disponible a: https://www.globalsuitesolutions.com/es/seguridad-informacion-iso-27001/
- *GlobalSuite Solutions* [en línia] [consulta: 27 d'abril de 2023]. Disponible a: https://www.globalsuitesolutions.com/es/cambios-norma-iso-27002-2022/
- *Secure&IT* [en línia] [consulta: 28 d'abril de 2023]. Disponible a: https://www.secureit.es/la-nueva-iso-270022022-cambios-y-periodo-de-adaptacion/?gclid=CjwKCAjws7WkBhBFEiwAIi1686fYmb_BLpxHGApyeWDV2kh2Jx2KyyoWmGpgl0VB4YyQ1Cy0PSMu8xoC2P4QAvD_BwE
- *ISO Tools* [en línia] [consulta: 29 d'abril de 2023]. Disponible a: https://www.isotools.us/2015/01/21/familia-normas-iso-27000/

- *ISO 27000* [en línia] [consulta: 29 d'abril de 2023]. Disponible a: https://www.iso27000.es/index.html
- *Normas ISO* [en línia] [consulta: 29 d'abril de 2023]. Disponible a: https://www.normas-iso.com/iso-27001/
- *IMSM* [en línia] [consulta: 2 de maig de 2023]. Disponible a: https://www.imsm.com
- *IMSM* [en línia] [consulta: 3 de maig de 2023]. Disponible a: https://www.imsm.com/es/iso-27001/
- *IMSM* [en línia] [consulta: 3 de maig de 2023]. Disponible a: https://www.imsm.com/es/wp-content/uploads/sites/12/2017/10/The-IMSM-Road-To-ISO-Implementation.pdf
- *NQA* [en línia] [consulta: 4 de maig de 2023]. Disponible a: https://www.nqa.com/es-es/certification/standards/iso-27001-2022
- *Industria Conectada 4.0* [en línia] [consulta: 4 de maig de 2023]. Disponible a: https://www.industriaconectada40.gob.es/difusion/Paginas/enlaces-interes.aspx
- *PQBWeb* [en línia] [consulta: 6 de maig de 2023]. Disponible a: https://www.pqbweb.eu/
- *Intercer* [en línia] [consulta: 6 de maig de 2023]. Disponible a: http://www.intercer.es/ISO%2037001.html
- *PQBWeb* [en línia] [consulta: 6 de maig de 2023]. Disponible a: https://www.pqbweb.eu/trainingPack-t-74v13-e-learning-iso-27001-training-package-readiness-and-audit-of-your-isms-version-2013.php
- *PQBWeb* [en línia] [consulta: 7 de maig de 2023]. Disponible a: https://www.pqbweb.eu/trainingPack-t-74v22-e-learning-iso-27001-training-package-readiness-and-audit-of-your-isms-version-2022.php
- *PQBWeb* [en línia] [consulta: 8 de maig de 2023]. Disponible a: https://www.pqbweb.eu/platform.php?i=&if=82&ch=2434
- *AENOR* [en línia] [consulta: 9 de maig de 2023]. Disponible a: https://revista.aenor.com/380/las-referencias-en-ciberseguridad-se-actualizan.html
- *PQBWeb* [en línia] [consulta: 9 de maig de 2023]. Disponible a: https://www.pqbweb.eu/page-news-on-iso-27001-version-2022-information-security-management-systems-requirements.php
- *ISO 27001* [en línia] [consulta: 14 de maig de 2023]. Disponible a: https://normaiso27001.es/

Punts de consulta generals:

- *Diccionari.cat* [en línia]. Disponible a: https://www.diccionari.cat/
- *Diccionaris.cat* [en línia]. Disponible a: https://www.diccionaris.cat/
- *Softcatalà* [en línia]. Disponible a: https://www.softcatala.org/corrector/
- *Cambridge Dictionary* [en línia]. Disponible a: https://dictionary.cambridge.org/
- *Webopedia* [en línia]. Disponible a: https://www.webopedia.com/

12. Annexos

En aquest apartat s'adjunta l'enllaç que permet la lectura de diversos documents pel que fa a aspectes de caràcter normatiu que es consideren rellevants. Per tal de poder visitar el primer i el segon enllaç, caldrà visitar la pàgina web i, posteriorment, en l'apartat "*Normas y Especificaciones de interés"* fer la descàrrega de les normatives que es desitgin consultar.

1. Tecnología de la información Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información Requisitos (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015)

2. Tecnología de la Información Técnicas de seguridad Código de prácticas para los controles de seguridad de la información (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015)

3. Nota de Prensa UNE Normalización Española