Resum Executiu

Autor: Marc Vilalta Parra
Àrea: Sistemes de Gestió de la Seguretat de la Informació
Data Lliurament: 9 de gener de 2023

Índex

1. Introducció

La informació és l'actiu més important del què disposa la nostra organització, i aquesta informació, diàriament està sotmesa a un gran número d'amenaces que poden comprometre la confidencialitat, integritat i disponibilitat d'aquesta. Així que hem de procurà protegir-la adequadament.

La millor manera de fer-ho és implementar un sistema altament comprovat i eficient, com és la implementació d'un Sistema de Gestió de Seguretat de la Informació (SGSI) basat en la norma ISO 27001.

2. Objectius

Protegir la informació.

Elaborar un Pla Director de Seguretat (PDS) que actualment no tenim.

Detectar i valorar els riscos de la nostra Organització, assegurant o minimitzant els impactes que poden tenir les amenaces sobre els nostre actius.

Generar confiança a treballadors, usuaris i tercers.

Treballar sobre el sistema de millora continua que estableix el mètode escollit

Optimitzar la realització de projecte futurs en l'àmbit de la seguretat de la informació i reduir-ne els costos.

3. Abast

Volem centrar l'abast en totes les àrees de l'organització, incloent els centres territorials i locals, des d'on oferim serveis als usuaris en relació a tots els processos i actius que tenen relació amb la seguretat de la informació.

4. Resultats

4.1 Anàlisi diferencial

Per tal de determinar quin és l'estat inicial de la seguretat i la normativa de l'Organització en relació a la seguretat de la informació fem un anàlisi diferencial sobre la norma ISO/IEC 27001 i els controls establerts a la ISO/IEC 27002.

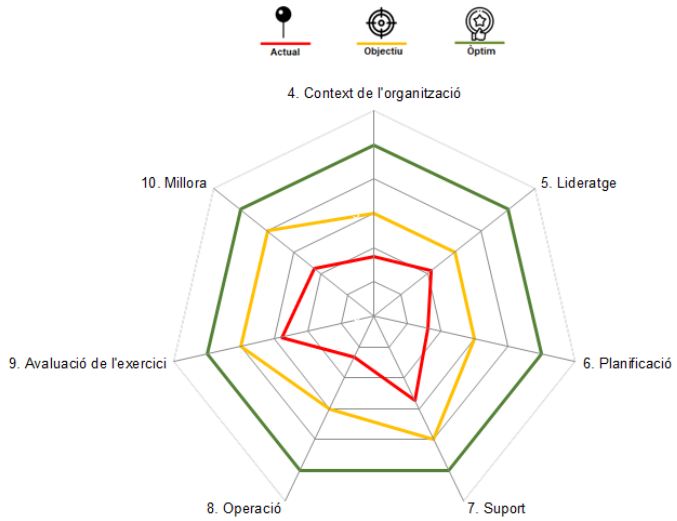
Aquest anàlisi es fa utilitzant un model de maduresa de les capacitats (CMM)

CMM	Significat	Descripció
L0	Inexistent	Carència completa de qualsevol procés que reconeguem.
		No s'ha reconegut que existeixi cap problema a resoldre.
L1	Inicial / Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal.
		Els procediments son inexistents o localitzats en àrees concretes.
		No existeixen plantilles definides a nivell corporatiu
L2	Reproduïble, però intuïtiu	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca.
		Es normalitzen les "bones practiques" en base a l'experiència i al mètode.
		No hi ha comunicació o entrenament formal, les responsabilitats queden a càrrec de cada individu.
		Es depèn del grau de coneixement de cada individu.
L3	Procés definit	La organització sencera participa al procés.
		Els processos estan implantats, documentats i comunicats mitjançant entrenament.
L4	Gestionat i mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos.
		Es disposa de tecnologia per automatitzar el flux de treball, s'ha de tenir eines per a millorar la qualitat i la eficiència.
L5	Optimitzat	Els processos estan sota constant millora.
		En base criteris quantitatius es determinen les desviacions més comunes i s'optimitzen els processos.

El resum de compliment de la norma per àrees de l'organització el trobem resumit en la següent Taula on també indiquem l'objectiu desitjable que ens hem fixat un cop realitzat el projecte.

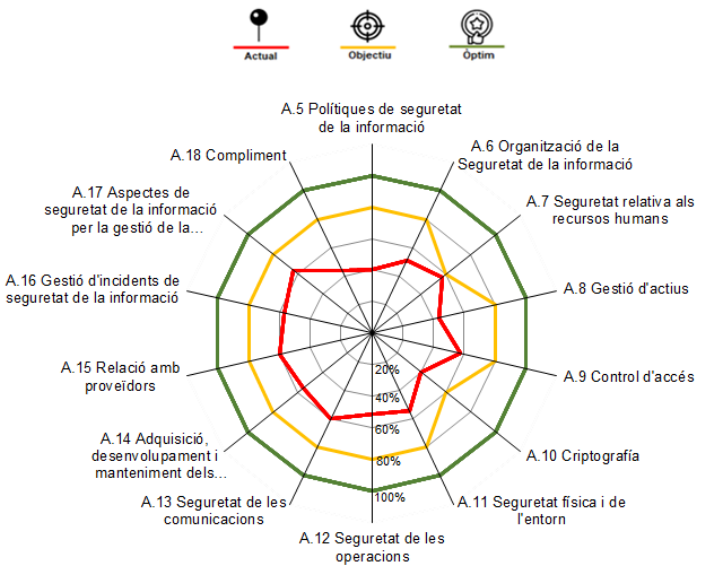
Control	CMM inicial	Compliment	Objectiu
4 L'Organització i el Context	1,75	No compleix	3
5 Lideratge	2,11	Compleix Parcialment	3
6 Planificació	1,60	No compleix	3
7 Suport	2,73	Compleix Parcialment	4
8 Operació	1,33	No compleix	3
9 Avaluació de l'exercici	2,78	Compleix Parcialment	4
10 Millora	2,25	Compleix Parcialment	4

Aquest valor els trobem representats gràficament en el diagrama següent on es poden observar les deficiències actuals, i es veu clarament que estem una mica allunyats dels objectius desitjables de l'Organització.



El mateix que hem fet per compliment de la norma, també ho fem per els controls definits en l'Annex A de la Norma ISO/IEC 27001 i que es troben desenvolupats a la ISO/IEC 27002, obtenint que:

Control	CMM inicial	Compliment	Objectiu
A.5 Polítiques de seguretat de la informació	2,00	Compleix Parcialment	4
A.6 Organització de la Seguretat de la informació	2,55	Compleix Parcialment	4
A.7 Seguretat relativa als recursos humans	2,83	Compleix Parcialment	3
A.8 Gestió d'actius	2,19	Compleix Parcialment	4
A.9 Control d'accés	2,87	Compleix Parcialment	4
A.10 Criptografia	2,00	Compleix Parcialment	3
A.11 Seguretat física i de l'entorn	2,72	Compleix Parcialment	4
A.12 Seguretat de les operacions	2,57	Compleix Parcialment	4
A.13 Seguretat de les comunicacions	3,00	Compleix però cal millorar	4
A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació	2,78	Compleix Parcialment	4
A.15 Relació amb proveïdors	3,00	Compleix però cal millorar	4
A.16 Gestió d'incidents de seguretat de la informació	2,86	Compleix Parcialment	4
A.17 Aspectes de seguretat de la informació per la gestió de la continuïtat del negoci	3,17	Compleix però cal millorar	4
A.18 Compliment	2,20	Compleix Parcialment	4



Tal i com passa amb la norma, en aquí també estem per sota l'objectiu fixat, no obstant podem observar que la situació és millor, ja que portem temps treballant en la qüestió de la seguretat.

Es pot observar que només en tres àrees complim amb la gestió de la seguretat de la informació, que corresponen en les àrees en les que s'han anat realitzant inversions en els darrers temps, com són, la seguretat en les comunicacions, la continuïtat de negoci i la relació amb els proveïdors, en la que s'està posant constant atenció.

4.2 Sistema de Gestió documental

Tot sistema de gestió de la seguretat es sustenta sobre una base documental que ens fa complir amb la normativa, en aquest cas la base documental que està establerta a la normativa ISO/IEC 27001 és la següent:

- **Política de Seguretat** que no és més que la normativa interna de l'organització en qüestió de compliment per part del personal afectat en tot l'abast del sistema de gestió de la seguretat de la informació.

- **Procediment d'auditories internes** és el procediment que han de seguir les auditories requerides per part de la normativa per tal d'anar revisant de forma constant el compliment i la millora del sistema de gestió de la seguretat de la informació.

- **Gestió d'indicadors** són els paràmetres que ens ajudaran a mesurar l'eficàcia dels controls existents i aplicats i poder establir així el nivell de maduresa.

- **Procediment de revisió per direcció** tot procediment definit ha d'estar validat i recolzat per la direcció de l'organització. El suport de la direcció es la clau per l'èxit en la implementació d'un sistema de gestió de la seguretat de la informació.

- **Gestió de rols i responsabilitats** tota implementació ha de comptar amb un equip que realitzi les tasques de creació, manteniment, supervisió i millora del sistema. Aquestes tasques es defineixen amb uns rols i unes responsabilitats que han d'estar clarament definides i consensuades amb la direcció de l'organització.

- **Metodologia d'anàlisi de riscos** és el mètode pel qual es valora quin es el risc que corren cadascun dels actius de l'organització en quant a seguretat de la informació, fent-ne una valoració i avaluant a quines amenaces i vulnerabilitats estan sotmesos i quin en seria l'impacte en cas de que aquestes es produïssin.

- **Declaració d'aplicabilitat** és el document en que es detallen els controls definits a la ISO/IEC 27001 i es determina quin és l'estat en que es troben i si s'aplica en l'abast definit inicialment del sistema de gestió de la seguretat de la informació.

4.3 Anàlisi de Risc

L'anàlisi del risc el realitzem utilitzant la metodologia Magerit que ens permet valorar econòmicament l'impacte que pot tenir per l'organització. L'anàlisi complert el podem trobar a la memòria del projecte. No obstant els resultats rellevants d'aquest anàlisi en quant a amenaces seria el següent:

- Les principal amenaça a la què està sotmesa l'organització és la falta de conscienciació i formació en qüestió de seguretat per part dels treballadors, voluntaris i altres que formen part de l'organització.
- La falta d'una metodologia que porti a una revisió i millora constant dels procediments que s'han anat establint en qüestions de seguretat i metodologies que han anat quedant obsoletes i antiquades davant l'evolució constant del procés de negoci i les tecnologies i amenaces actuals.
- La seguretat i confidencialitat de les dades i les infraestructures també han sortit assenyalades en aquest anàlisi.
- La telefonía mòbil és un altre punt feble de la nostre organització, la seguretat, la falta de traçabilitat i de confidencialitat en cas d'incident és un problema important.
- Altres riscos detectats venen derivats de falta de classificació dels actius i d'un seguiment i control d'aquests.

4.4 Proposta de Projectes

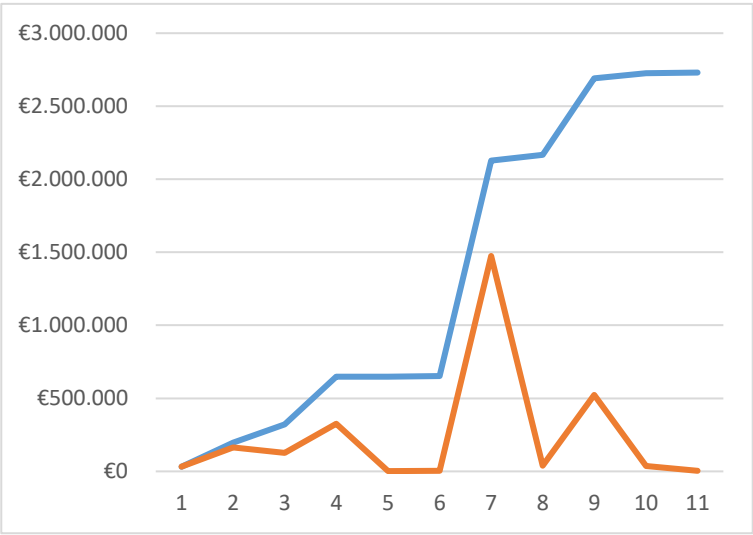
Del resultat de l'anàlisi de riscos anterior en sorgeixen una sèrie de projectes que caldria realitzar per tal d'assolir els objectius plantejats a l'inici. Aquests projectes juntament amb la realització d'aquest treball ens faran avançar en aquest objectiu.

Els projectes que plantegem requereixen d'una gran inversió, no obstant el ROI que n'esperem és alt, tot i que no podem fer-ne una valoració econòmica exacte degut a la tipologia de projectes que presentem, que són els següents:

- Campanya de conscienciació sobre la seguretat en els sistemes d'informació a l'organització.
- Formacions sobre l'ús de les eines informàtiques comuns a l'organització.
- Formació i cursos especialitzats per Administradors de sistema.
- Implantació d'un nou sistema antivirus de nova generació.
- Revisió i millora del sistema de copies de seguretat.
- Revisió i millores del control d'accessos a àrees segures.
- Implementació d'un MDM per la telefonía mòbil.
- Revisió i actualització dels procediments del departament de SI.
- Nous procediments SI.
- Gestió d'actius.
- Procediments per la contractació de personal.

El costos d'aquests projectes els trobem en els quadres i gràfics que trobem a continuació i serien els corresponents al 2023.

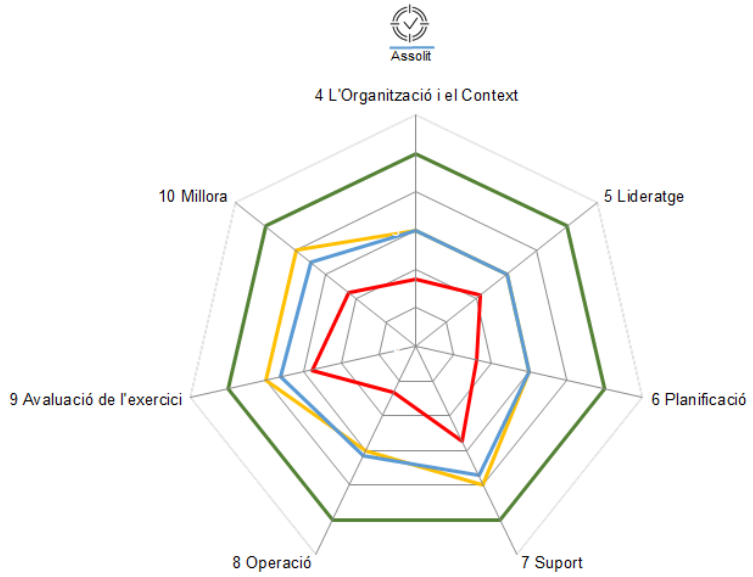
Projecte	Cost del projecte	Cost acumulat
Projecte 1	31.710 €	31.710 €
Projecte 2	163.910 €	195.620 €
Projecte 3	126.540 €	322.160 €
Projecte 4	325.250 €	647.410 €
Projecte 5	1.800 €	649.210 €
Projecte 6	3.700 €	652.910 €
Projecte 7	1.474.620 €	2.127.530 €
Projecte 8	38.970 €	2.166.500 €
Projecte 9	523.550 €	2.690.050 €
Projecte 10	37.010 €	2.727.060 €
Projecte 11	3.250 €	2.730.310 €



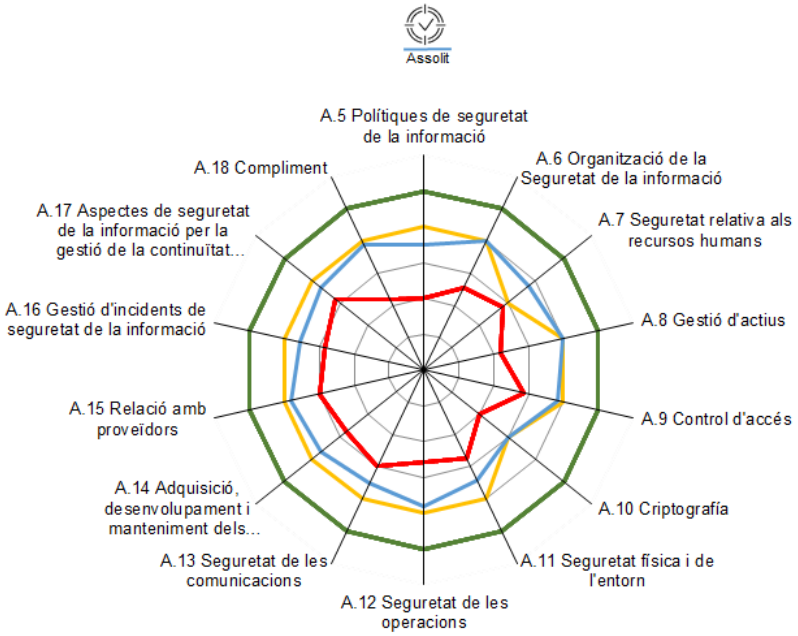
4.5 Auditoria de Compliment

Un cop s'hagin realitzat els projectes anteriors la previsió del nivell de maduresa de la norma i els controls de la ISO/IEC 27001 quedaria de la següent manera:

Control	CMM actual	Compliment	Objectiu
4 L'Organització i el Context	3,00	Compleix però cal millorar	3
5 Lideratge	3,00	Compleix però cal millorar	3
6 Planificació	3,00	Compleix però cal millorar	3
7 Suport	3,73	Compleix	4
8 Operació	3,17	Compleix però cal millorar	3
9 Avaluació de l'exercici	3,61	Compleix	4
10 Millora	3,50	Compleix	4



Control	CMM actual	Compliment	Objectiu
A.5 Polítiques de seguretat de la informació	**3,50**	Compleix	**4**
A.6 Organització de la Seguretat de la informació	**4,00**	Bon nivell de compliment	**4**
A.7 Seguretat relativa als recursos humans	**3,75**	Compleix	**3**
A.8 Gestió d'actius	**4,00**	Bon nivell de compliment	**4**
A.9 Control d'accés	**3,83**	Compleix	**4**
A.10 Criptografia	**3,00**	Compleix però cal millorar	**3**
A.11 Seguretat física i de l'entorn	**3,42**	Compleix	**4**
A.12 Seguretat de les operacions	**3,82**	Compleix	**4**
A.13 Seguretat de les comunicacions	**3,50**	Compleix	**4**
A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació	**3,67**	Compleix	**4**
A.15 Relació amb proveïdors	**3,83**	Compleix	**4**
A.16 Gestió d'incidents de seguretat de la informació	**3,57**	Compleix	**4**
A.17 Aspectes de seguretat de la informació per la gestió de la continuïtat del negoci	**3,67**	Compleix	**4**
A.18 Compliment	**3,90**	Compleix	**4**



Com podem comprovar en les taules i gràfiques anteriors els resultat esperats són molt bons però sense acabar d'assolir els objectius marcats.

5. Conclusions

Amb la realització d'aquest treball es pretenia avançar en la millora de l'organització i dotar de un nivell de seguretat suficient a la informació de l'organització. Dona confiança i un bon servei a administracions i usuaris és la nostra prioritat.

Tot i els esforços i inversions en seguretat realitzats fins ara, faltava realitzar una passa més, i seguir un mètode com el que proposa la Norma ISO 27001, tot i que comporta un gran esforç ens garanteix uns resultats més acurats i evita treballs i inversions innecessàries i més adaptades a la realitat, en definitiva fa mes eficient els treballs i les actuacions a realitzar.

Amb el treball realitzat i els projecte proposats creiem assolir gran part de l'objectiu inicial d'aquest treball, on s'han fet tots els passos per la implementació d'un SGSI seguint la indicacions de la Norma ISO 27001, dic gran part i no tots els objectius, perquè ens havíem marcat un objectius de maduresa per els controls una mica ambiciosos, i no hem aconseguit arribar a aquests objectius, tot i que ens hi hem quedat molt a prop.

No obstant no haver acabat assolint tots els objectius fixats en un inici, el sistema de millora constant que proposa el mètode implementat, farà que aquests s'aconsegueixin en breu. Inclús millorar els resultats esperats. Per això cal dotar

dels recursos necessaris per la realització dels projectes, aquesta metodologia ens garanteix que les inversions seran eficaces i no estaran per sobre de les necessitats requerides, sabem que formem part d'una ONG i els recursos son limitats.

Formar el personal que realitzarà aquestes tasques és una de les claus d'aquest projecte, juntament amb el compromís de tots.

Un cop finalitzats els projectes exposats caldria encarregar una auditoria externa per tal de validar tot l'estudi realitzat i valorar el procés iniciat.