



Implementació d'un SGSI en una cooperativa

PRESENTACIÓ DE TREBALL FINAL DE MÀSTER

Màster Universitari en Ciberseguretat i Privadesa

Adrià Sànchez Falcó



CONTINGUTS

01

Introducció i
motivació

02

Fases del
projecte

03

Context de
l'organització

04

Gestió
Documental

05

Anàlisi de
Riscos

06

Propostes de
Projectes

07

Auditoria de
Compliment

08

Conclusions





01

INTRODUCCIÓ I MOTIVACIÓ

INTRODUCCIÓ I MOTIVACIÓ



LA SEURETAT DE LA INFORMACIÓ

- El entorns digitals formen un actiu crític.
- Protegir la Confidencialitat, Integritat i Disponibilitat de la informació.



SECTOR AGROALIMENTARI

- La digitalització dels processos crea nous riscos de seguretat.
- Necessitat d'un Pla Director de Seguretat.



OBJECTIUS



Millorar la seguretat d'una cooperativa

Implantant un SGSI amb estàndards internacionals ISO/IEC 27001 i 27002.



Proporcionar valor

Una protecció adequada de dades sensibles que augmenti la confiança dels clients i parts interessades.



Beneficiar els actors implicats

Millorar la reputació, la conformitat i la conscienciació dels empleats.



METODOLOGIA

ISO/IEC 27001

Estàndard internacional que estableix requisits per a la implementació, manteniment i millora continua del SGSI.

ISO/IEC 27002

Proporciona directrius per a la implementació de controls de seguretat de la informació agrupats en 4 dominis.



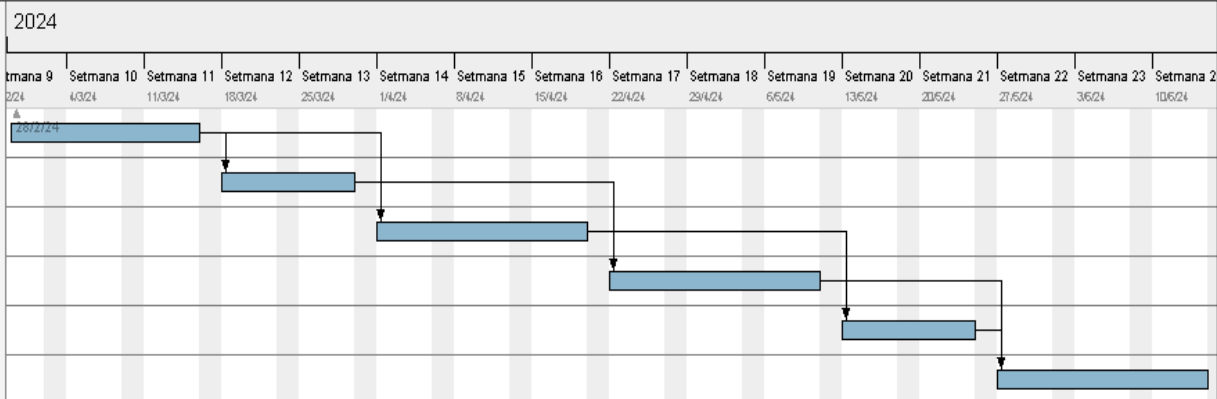


02

FASES DEL PROYECTO



Nom	Inici	Finalització
Fase 1: Contextualització, objectius i anàlisi diferencial	28/2/24	15/3/24
Fase 2: Sistema de Gestió Documental	18/3/24	29/3/24
Fase 3: Elaboració metodologia Anàlisi de riscos	1/4/24	19/4/24
Fase 4: Proposta de projectes	22/4/24	10/5/24
Fase 5: Auditoria de compliment de la ISO	13/5/24	24/5/24
Fase 6: Presentació de resultats i entrega	27/5/24	14/6/24





03

CONTEXT DE L'ORGANITZACIÓ

La cooperativa

Com és?

- Una cooperativa agrícola d'arròs.
- Distribuidora nacional i internacional.
- Més de 2.500 socis i 60 treballadors.

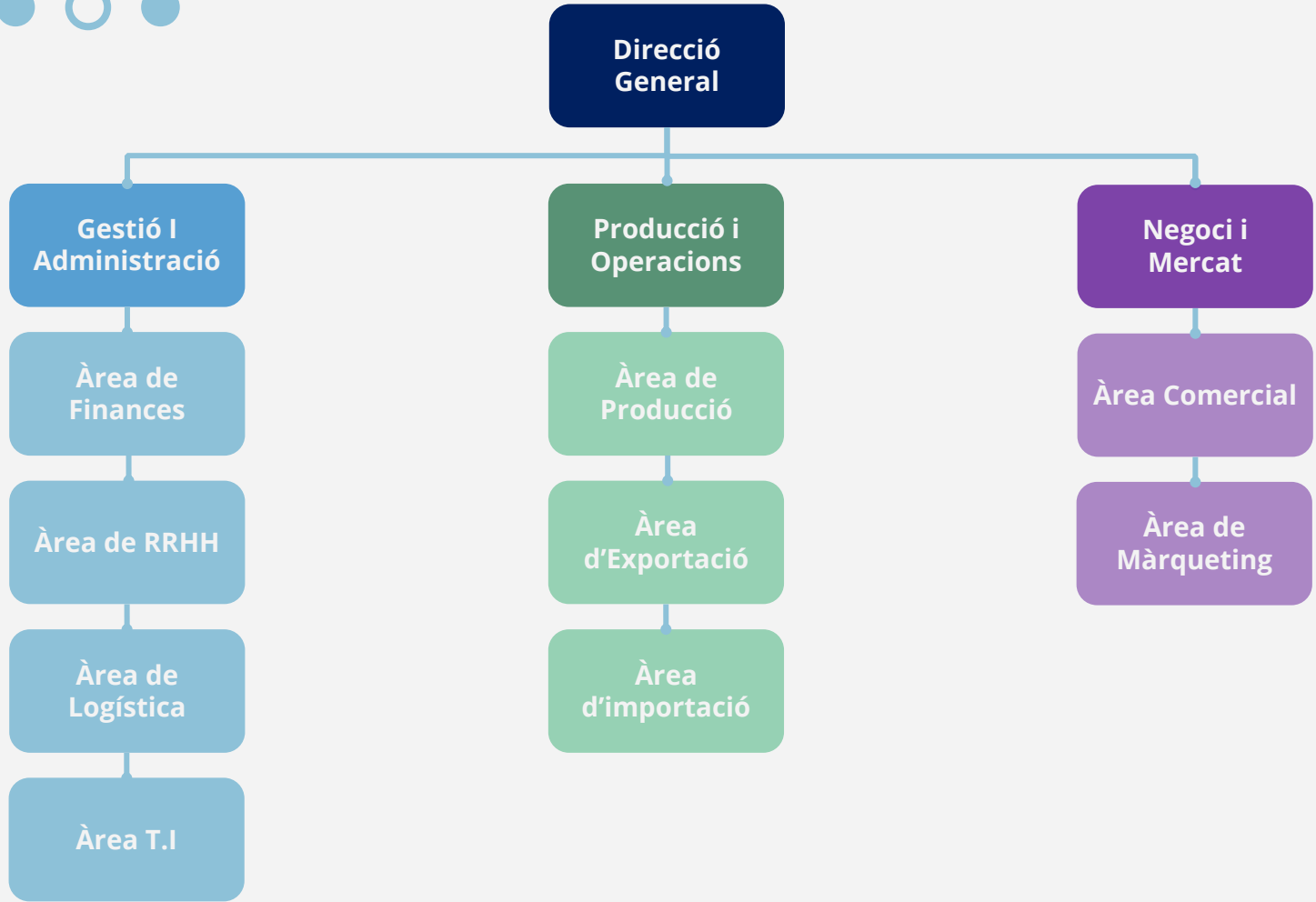
Reconeixement

- Compromís amb la qualitat, sostenibilitat i la comunitat agrícola.
- Participació en fires i esdeveniments sectorials.

Digitalització

- Sistemes de gestió de la cadena d'aprovisionament.
- Plataformes de comerç electrònic.
- Solucions de comunicació interna.







Situació actual

Debilitats

- No disposa d'un SGSI
- Manca de formació en seguretat de la informació.
- Sistemes informàtics antiquats.

Amenaces

- Increment de les amenaces cibernètiques.
- Canvis en la legislació de protecció de dades.
- Competència en el sector agrícola.

Fortaleses

- Reputació en el sector agrícola.
- Recursos financers per invertir.
- Suport de la comunitat agrícola.

Oportunitats

- Millorar la confiança dels clients.
- Creixement i expansió.
- Eficiència operativa.

Anàlisi Diferencial

Efectivitat	CMM	Valor	Significat	Descripció
0%	L0	0	Inexistent	No hi ha cap procés reconegut. No s'ha identificat cap problema a resoldre.
10%	L1	1	Inicial / Ad-hoc	Els èxits depenen de l'esforç personal. Procediments inexistents o locals. No hi ha plantilles corporatives definides.
50%	L2	2	Reproduïble, però intuïtiu	Processos similars es fan de manera semblant per diferents persones. Bones pràctiques basades en l'experiència. No hi ha entrenament formal.
90%	L3	3	Procés definit	Tota l'organització participa. Processos implantats, documentats i comunicats amb entrenament.
95%	L4	4	Gestionat i mesurable	Seguiment amb indicadors numèrics i estadístics. Tecnologia per automatitzar fluxos de treball i millorar qualitat i eficiència.
100%	L5	5	Optimitzat	Processos en constant millora. Optimització basada en criteris quantitius per reduir desviacions comunes.

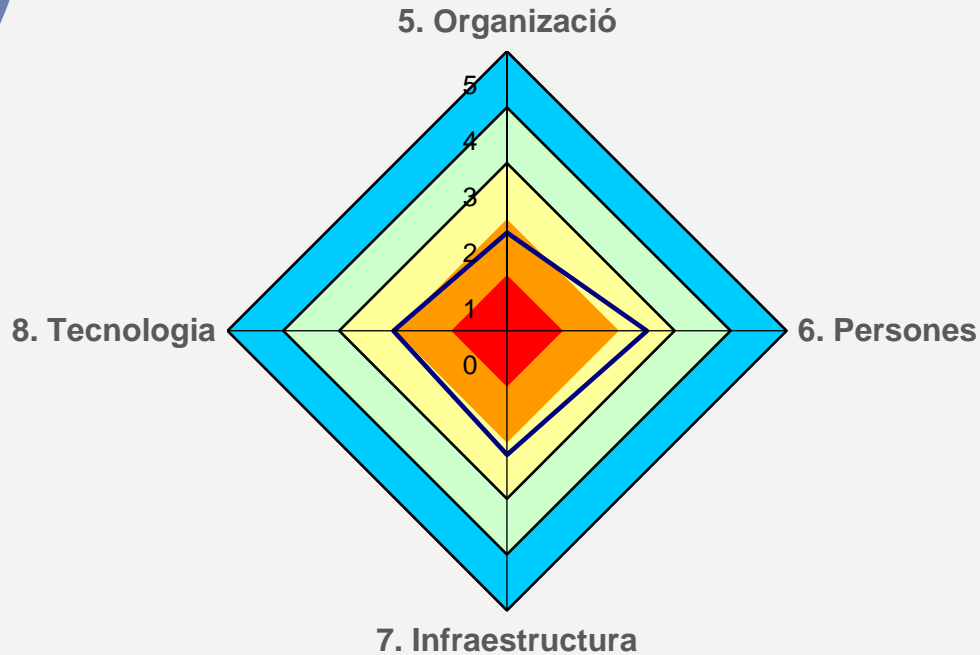
Nivell actual de compliment ISO 27001



Mesures ISO 27001	Maduresa inicial
4. Contexte organitzacional	L1 - 1,75
5. Lideratge	L1 - 1,66
6. Planificació	L1 - 1,77
7. Suport	L2 - 2,26
8. Operació	L1 - 1
9. Avaluació de l'exercici	L1 - 1
10. Millora	L1 - 1



Nivell actual dels controls ISO 27002



Mesures ISO 27002	Maduresa inicial
5. Organització	L1 - 1,76
6. Persones	L2 - 2,50
7. Infraestructura	L2 - 2,21
8. Tecnologia	L2 - 2,03

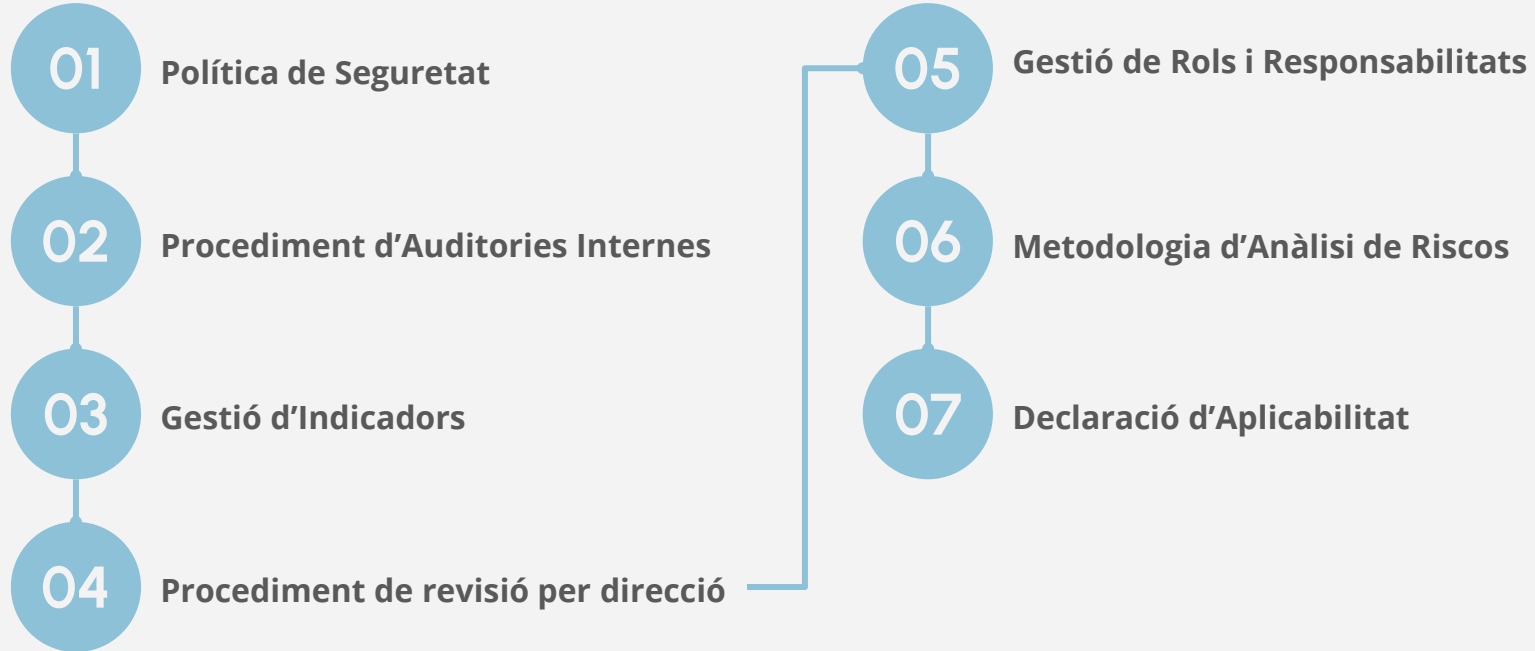


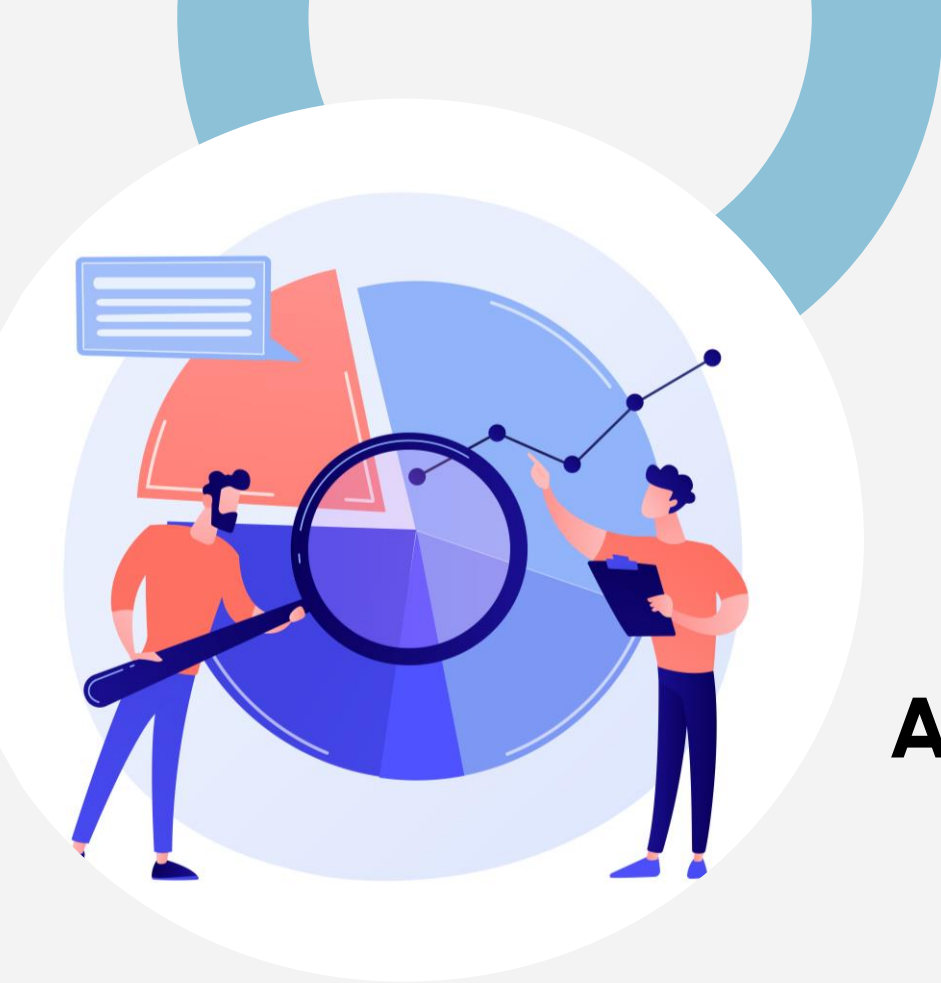


04

GESTIÓ DOCUMENTAL

Sistema de Gestió Documental





05

ANÀLISIS DE RISCOS



Anàlisi i valoració d'actius

Escala de valors per dimensió

10	Molt Alta (MA)	Dany molt greu a la cooperativa
7 – 9	Alta (A)	Dany greu a la cooperativa
4 – 6	Mitjana (M)	Dany important a la cooperativa
1 – 3	Baixa (B)	Dany menor a la cooperativa
0	Molt baixa (MB)	Irrellevant a efectes pràctics

Dades

Hardware

Aplicacions
informàtiques

Claus
Criptogràfiques

Xarxes
comunicació

Instal·lacions

Suports
d'informació

Equipament
auxiliar

Serveis



Anàlisi d'amenaques



Desastres Naturals

Incendis forestals, inundacions, terratrèmols o tempestes.



Errors i fallades no intencionades

Errors causats per persones en l'ús, la configuració o gestió de sistemes informàtics.



Origen Industrial

Fallades en equips, interrupcions en el subministrament elèctric, condicions ambientals inadequades o similars.



Atacs intencionats

Credencials robades, distribució de programari maliciós, intents d'accés no autoritzat o similars.



Valoració de l'impacte, risc i accions

Actiu	Valor	Amenaça	Prob	Degradació	Impacte	Risc Inicial	Acció	Risc residual	
(D) Informació dels membres	8,4	N.1	Foc	0,1	100%	8,4	0,84	Assumir	-
		N.2	Danys per aigua	0,1	75%	6,3	0,63	Assumir	-
		E.1	Error d'usuari	5	25%	2,1	10,5	Assumir	-
		E.2	Error d'administrador	5	50%	4,2	21	Mitigar	6,3
		E.15	Alteració accidental de la informació	7,5	50%	4,2	31,5	Mitigar	9,45
		E.18	Destrucció de la informació	7,5	75%	6,3	47,25	Mitigar	14,175
		E.19	Fuga de informació	10	70%	4,2	42	Evitar	12,6
		A.4	Manipulació de la informació	5	75%	6,3	31,5	Mitigar	9,45
		A.5	Suplantació d'identitat	7,5	75%	6,3	47,25	Evitar	14,175
		A.6	Abús de privilegis d'accés	5	75%	6,3	31,5	Mitigar	9,45
		A.11	Accés no autoritzat	5	75%	6,3	31,5	Evitar	9,45
		A.15	Modificació deliberada de la informació	5	75%	6,3	31,5	Mitigar	9,45
		A.18	Destrucció de la informació	7,5	100%	8,4	63	Mitigar	18,9
		A.19	Divulgació de informació	5	75%	6,3	31,5	Mitigar	9,45



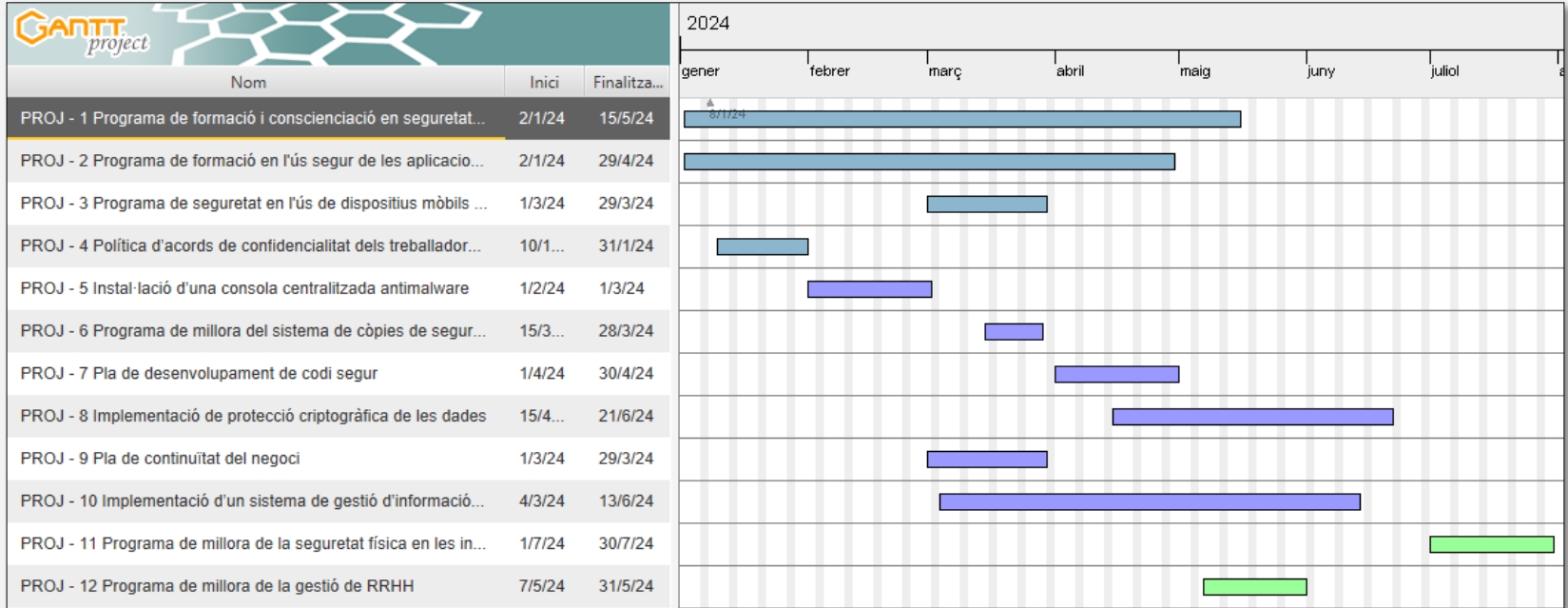
06

PROPOSTES DE PROJECTES

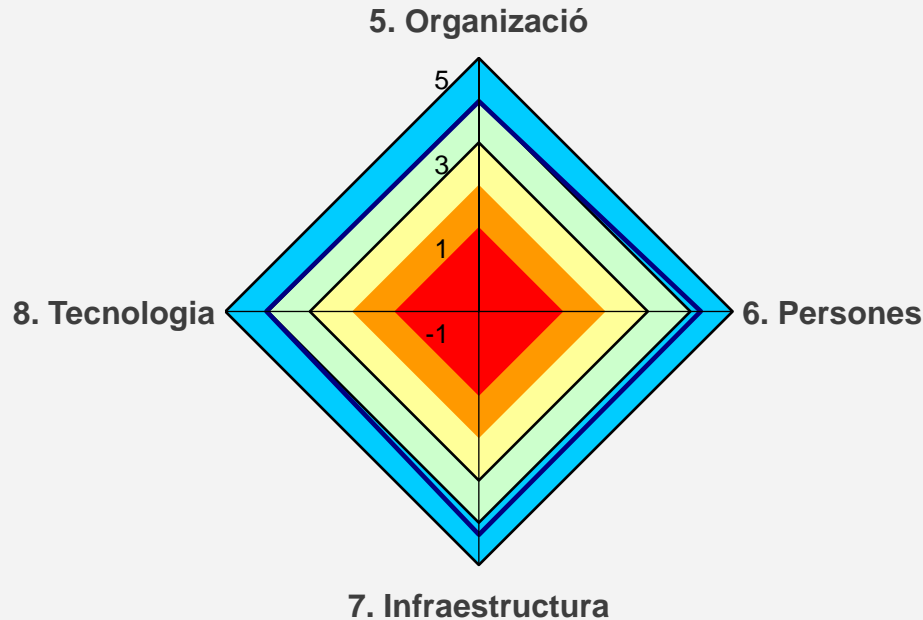
Estructura de projecte

Codi	Nom	
Pressupost (€)	Planificació	Prioritat (1 - 10)
Objectiu		
Descripció		
Controls ISO 27002		
Amenaces tractades	Actius afectats	
Responsable	Membres implicats	

Llista de projectes



RESULTATS ESPERATS



- Disminuir el nivell de risc acceptable.
- Controls ISO 27002 >= Gestionat i Mesurable
- Millora estable dels 4 dominis.





07

AUDITORIA DE COMPLIMENT

Característiques de l'auditoria

Objectiu

- Avaluar el compliment de les bones pràctiques ISO 27001 i 27002.
- Assegura la correcta implementació del SGSI.
- Avaluar la maduresa final.

Tipus

- Auditoria Interna
- Basa en la normativa ISO/IEC 27001 i 27002 (2023).

Procediment

- Planificació del calendari.
- Reunions preparatòries.
- Treball de camp.
- Consolidació de resultats.



Avaluació de maduresa ISO 27001

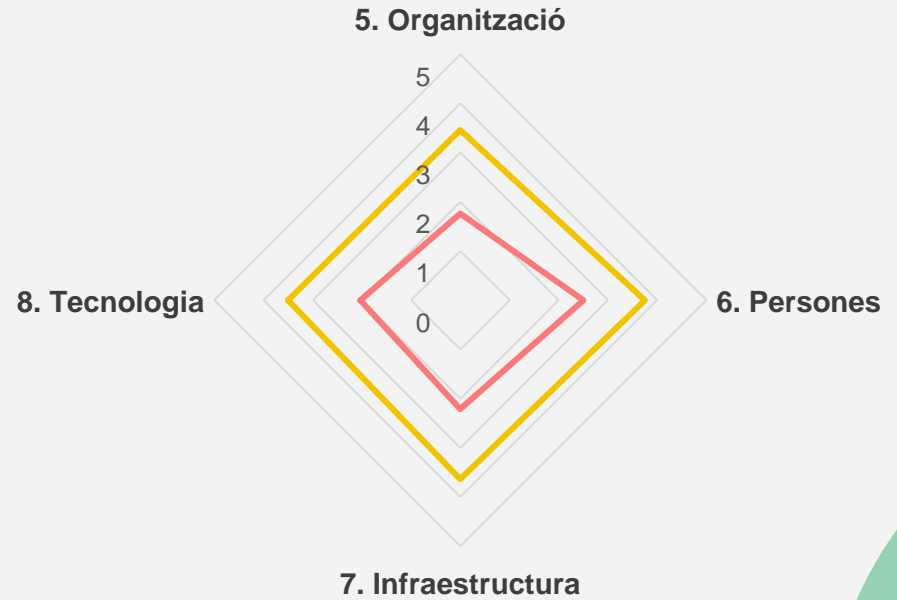
Mesures ISO 27001	Maduresa inicial	Maduresa actual	Objectiu
4. Context organitzacional	L1 - 1,75	L3 - 3,75	L4 - 4
5. Lideratge	L1 - 1,66	L3 - 3,67	L4 - 4
6. Planificació	L1 - 1,77	L3 - 3,87	L4 - 4
7. Suport	L2 - 2,26	L3 - 3,6	L4 - 4
8. Operació	L1 - 1	L3 - 3,67	L4 - 4
9. Avaluació de l'exercici	L1 - 1	L4 - 4	L4 - 4
10. Millora	L1 - 1	L3 - 3,5	L4 - 4



Maduresa assolida controls ISO 27002

Dominis ISO 27002	Maduresa inicial	Maduresa actual	Objectiu
5. Organització	L1 - 1,76	L3 - 3,46	L4 - 4
6. Persones	L2 - 2,50	L3 - 3,75	L4 - 4
7. Infraestructura	L2 - 2,21	L3 - 3,64	L4 - 4
8. Tecnologia	L2 - 2,03	L3 - 3,5	L4 - 4

— Maduresa inicial — Maduresa actual





08

CONCLUSIONS





Anàlisi de Riscos

Fonamental per a prendre decisions sobre la seguretat de la informació.



Mitigació d'amenaques

S'han aconseguit mitigar amenaces i vulnerabilitats que afecten als actius.



Pla Director de Seguretat

La seva elaboració estableix una base sòlida que fa de guia en la planificació de la seguretat de la informació.



Millora Continua

S'ha de seguir treballant per a mantenir el nivell de maduresa el més òptim possible.



Objectius assolits

S'ha millorat la seguretat, i això li aportaria més valor i beneficiaria els actors implicats.



Aprenentatge personal

Millor comprensió de la seguretat de la informació i d'un SGSI, sobre la teoria prèviament estudiada.



GRÀCIES PER L'ATENCIÓ

PRESENTACIÓ DE TREBALL FINAL DE MÀSTER

Màster Universitari en Ciberseguretat i Privadesa

Adrià Sánchez Falcó

