# Implementació d’un SGSI en una cooperativa

**Nom Estudiant:** Adrià Sànchez Falcó

**Programa:** Màster Universitari en Ciberseguretat i Privadesa (MUCIP)
**Àrea:** Sistemes de Gestió de la Seguretat de la Informació

**Consultor:** Igor Ruiz Agúndez
**Professor responsable de l’assignatura:** Carles Garrigues Olivella
**Centre:** Universitat Oberta de Catalunya

**Data Lliurament:** 14 de juny del 2024

**FITXA DEL TREBALL FINAL**

| | |
|---|---|
| **Títol del treball:** | *Implementació d'un SGSI en una cooperativa* |
| **Nom de l'autor:** | *Adrià Sànchez Falcó* |
| **Nom del consultor/a:** | *Igor Ruiz Agúndez* |
| **Nom del PRA:** | *Carles Garrigues Olivella* |
| **Data de lliurament (mm/aaaa):** | *06/2024* |
| **Titulació o programa:** | Màster Universitari en Ciberseguretat i Privadesa (MUCIP) |
| **Àrea del Treball Final:** | *Sistemes de Gestió de la Seguretat de la Informació* |
| **Idioma del treball:** | *Català* |
| **Paraules clau** | *ISO 27001, SGSI, Seguretat* |


**Resum del Treball (màxim 250 paraules):** *Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball*

L'objectiu d'aquest Treball Final de Màster és implementar un Sistema de Gestió de la Seguretat de la Informació (SGSI) en una cooperativa agrícola fictícia. La seguretat de la informació és fonamental per a aquesta organització, atès que gestiona dades sensibles de clients i empleats, i està subjecta a regulacions de protecció de dades.

El SGSI en l'empresa funciona com a un conjunt de polítiques basat en els estàndards internacionals ISO/IEC 27001 i 27002 (2023), així com la Metodologia d'Anàlisi i Gestió de Riscos de MAGERIT, que permeten realitzar una avaluació exhaustiva dels riscos i una identificació dels actius crítics, seguit per la implementació de controls de seguretat i la formació del personal.

El projecte s'ha estructurat en sis fases, començant per la contextualització i definició d'objectius, seguit per la creació d'un sistema de gestió documental, la identificació i valoració dels riscos, la proposta de projectes per mitigar aquests riscos, una auditoria de compliment de la ISO i la presentació dels resultats.

Els resultats es troben visibles, mostrant un anàlisi de riscs, unes propostes de projectes i una primera auditoria de compliment com a parts més contundents respecte a les millores de seguretat de la informació de l'empresa.

Com a conclusió, implantar un SGSI és una inversió crucial, i la direcció de la cooperativa ha pres una decisió encertada en adoptar aquest sistema, ja que la seva desatenció podria haver desembocat en conseqüències costoses.

**Abstract (in English, 250 words or less):**

The purpose of this Master's Thesis is to implement an Information Security Management System (ISMS) in a fictitious agricultural cooperative. Information security is paramount for this organization, as it manages sensitive data of clients and employees and is subject to data protection regulations.

The ISMS in the company functions as a set of policies based on the international standards ISO/IEC 27001 and 27002 (2023), as well as the Risk Analysis and Management Methodology for Information Systems (MAGERIT), enabling a comprehensive assessment of risks and identification of critical assets, followed by the implementation of security controls and staff training.

The project has been structured into six phases, starting with contextualization and goal definition, followed by the creation of a document management system, risk identification and assessment, proposal of projects to mitigate these risks, an ISO compliance audit, and presentation of the results.

The results are evident, showcasing a risk analysis, project proposals, and an initial compliance audit as the most robust parts concerning the improvements in the company's information security.

In conclusion, implementing an ISMS is a crucial investment, and the cooperative's management has made the right decision in adopting this system, as neglecting it could have led to costly consequences.

# Índex

# Figures i taules

## Índex de figures



## Índex de taules

# 1. Introducció

## 1.1 Context i justificació del Treball

La seguretat de la informació és una preocupació fonamental per a qualsevol empresa actualment. Els entorns digitals formen un actiu crític, i la seva protecció adequada és indispensable per preservar la integritat, la confidencialitat i la disponibilitat dels recursos empresarials. Per tant, la seguretat deixa de ser un aspecte opcional i passa a ser ineludible per a tota organització.

En aquest treball s'escull el cas d'una cooperativa agrícola que agrupa més de 2.500 socis dedicats al cultiu, processament i comercialització de l'arròs i que es mantenen fidels als valors centrals de qualitat, sostenibilitat i compromís amb la comunitat agrícola. La indústria agroalimentària s'identifica com un sector crític, i és un sector subjecte a regulacions específiques que protegeixen la producció, manipulació i distribució d'aliments, així com normatives amb protecció de dades i seguretat alimentària.

La cooperativa regula la recopilació, emmagatzematge i ús de la informació personal dels clients i empleats. Per tant, la llei que ho regula és la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD). Aquesta llei complementa el Reglament General de Protecció de Dades (RGPD) de la Unió Europea i estableix les regles específiques que les organitzacions han de seguir en el tractament de les dades personals.

Pel que fa a la ciberseguretat, com a empresa del sector agrícola i alimentari, estan exposats a amenaces en línia. Millorar l'accés a Internet facilita que les empreses agrícoles adoptin eficiències i redueixin els costs a través de tecnologia millorada, però també amplia la superfície de ciberatacs i el panorama de les amenaces. La manipulació de dades sensibles dels clients, així com la gestió adequada de les operacions internes de l'empresa es presenta com una tasca crítica. A més, la manca d'un marc integral de seguretat de la informació deixaria la cooperativa vulnerable a possibles violacions de seguretat, que podrien comprometre la confiança del client, afectar la reputació de la marca i ocasionar pèrdues financeres significatives.

Segons el lloc web Artica[1], la ciberseguretat és un aspecte crític per a la indústria agroalimentària, ja que els avenços en tecnologies digitals poden augmentar la vulnerabilitat a ciberatacs. La digitalització dels processos agrícoles, com l'ús de sensors i la recopilació de dades en temps real aporten grans avantatges en la millora de la productivitat, però també crea nous riscos de seguretat. Els dispositius agrícoles connectats a Internet poden ser objectius de ciberdelinqüents, posant en perill la confidencialitat de les dades i la integritat dels sistemes agrícoles. D'altra banda, els ciberatacs a la cadena d'aprovisionament poden tenir repercussions greus en la seguretat alimentària global. És imprescindible que les empreses agrícoles adoptin mesures de protecció adequades per mitigar aquests riscos i assegurar la continuïtat de les seves operacions.

El Pla Director de seguretat és una eina obligatòria per al responsable de la Seguretat de la informació de l'entitat, perquè a través d'aquest full de ruta l'empresa pot gestionar de forma adequada la seguretat. Per tant, el projecte planteja l'establiment de les bases per a la implementació d'un SGSI (Sistema de Gestió de la Seguretat de la Informació).

**Motivació per a implementar un SGSI**

Com a empresa que opera en el sector de l'alimentació, la cooperativa gestiona informació sensible relacionada amb la producció, distribució i comercialització d'arròs. La implementació d'un SGSI garantirà la protecció d'aquesta informació contra amenaces com la pèrdua de dades, l'accés no autoritzat i el robatori d'informació.

D'altra banda, molts clients i socis comercials de la cooperativa poden requerir garanties de seguretat de la informació com a part dels seus acords comercials. Un SGSI ben implementat pot ser un factor clau per mantenir i ampliar aquestes relacions comercials. A més és crucial per a la cooperativa complir amb els requisits legals i normatius vigents. La implementació d'un SGSI ajudarà a garantir que l'empresa compleixi amb aquests requisits i eviti sancions i multes.

[1] Fresno, J.M. [José Manuel]. (6 de gener, 2024). Ciberseguridad en la industria agroalimentària. *ARTICA* [en línia]. https://www.articai.es/ciberseguridad-en-la-industria-agroalimentaria/

## 1.2 Objectius del Treball

### 1. Proporcionar valor a l'empresa:

La cooperativa agrícola, com a primer sector industrial de la economia del país, ha de fer un pas endavant en la seguretat de la informació elaborant un pla d'implementació d'un Sistema de Gestió de Seguretat de la Informació (SGSI) que garanteixi la protecció adequada de les dades sensibles i el compliment de les regulacions legals i normatives. També s'ha d'augmentar confiança dels clients i altres parts interessades mitjançant la implementació dels estàndards internacionals ISO/IEC 27001 i 27002, que especifiquen els requisits per a la gestió efectiva de la seguretat de la informació.

### 2. Millorar la seva seguretat:

Mitjançant l'ús d'eines com la Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes d'Informació (MAGERIT), identificarem les àrees més vulnerables i adoptarem les mesures tècniques necessàries per corregir-les. Això ens permetrà complir amb les normatives internacionals i establir un procés de millora continua (PDCA) per al pla de seguretat.

### 3. Beneficiar els actors aplicats:

Millorarem la reputació, la confiança dels clients i la conformitat amb les normatives legals. Assegurant als clients una major protecció de les seves dades personals i una relació més segura amb la cooperativa. A més, els empleats també veuran incrementada la seva consciència i capacitació en seguretat de la informació, garantint una millor gestió dels recursos digitals i reduint el risc d'incidents de seguretat.

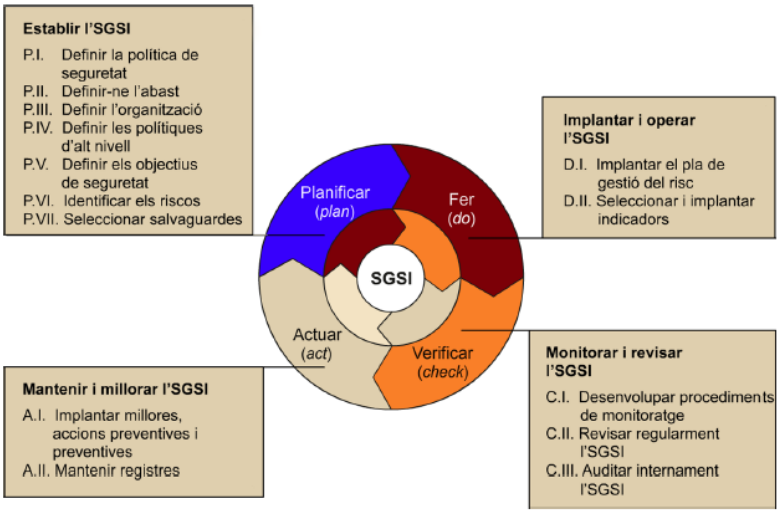


Figura 1. Cicle de Deming PDCA aplicat al SGSI

Per tant, aquest Pla Director de Seguretat (PDS) de la cooperativa d'arròs abasta una sèrie de mesures, processos i pràctiques destinades a protegir la informació i els recursos digitals de l'organització, assegurant al mateix temps la seva disponibilitat i integritat enfront de les amenaces de seguretat cada vegada més sofisticades. L'enfocament del PDS es centra en totes les àrees de l'organització, incloent-hi la seu central, la planta de processament i la oficina territorial. Aquest enfocament integral garanteix que cap aspecte de l'activitat empresarial quedi sense protecció, assegurant una gestió eficaç de la seguretat de la informació en tots els fronts possibles.

### 1.3 Enfocament i mètode seguit

El plantejament del projecte és establir les bases d'un Pla Director de Seguretat per a la cooperativa. El procés s'efectuarà a través d'aquestes etapes:

- Analitzar i detallar l'inventari d'actius de l'empresa identificant tots els recursos crítics per al funcionament i la seguretat de la informació.
- Estudiar les amenaces a les quals l'empresa està exposada, incloent-hi factors com ciberatacs, errors humans i desastres naturals.
- Avaluar l'impacte potencial d'aquestes amenaces en els actius de l'empresa, tant en termes de pèrdua financera com de danys a la reputació.
- Proposar un pla d'acció per abordar les amenaces identificades, incloent-hi la implementació de controls de seguretat i la formació del personal.
- Avaluar l'impacte residual després de l'aplicació del pla d'acció, per assegurar que s'han reduït adequadament els riscos.

Per aportar informació addicional, cal destacar el paper clau del personal de Tecnologies de la Informació (T.I) en la implementació del Pla Director de Seguretat de la cooperativa. Aquest personal té la responsabilitat de garantir la continuïtat de les operacions tecnològiques de l'empresa i de seguir les directrius establertes pel Pla Director de Seguretat. Ignorar aquesta responsabilitat podria resultar en una falta de cohesió en la implementació del SGSI, podent generar un augment de la càrrega de treball i ineficiències.

Les normes ISO/IEC 27001 i 27002 són estàndards internacionals que se centren en la gestió de la seguretat de la informació dins una organització. Com

són reconegudes a escala mundial i establertes com a referència, són les que escullo per al desenvolupament del SGSI de la cooperativa.

L'ISO/IEC 27001 estableix els requisits per establir, implementar, mantenir i millorar contínuament un sistema de gestió de seguretat de la informació (SGSI).
En el cas de la cooperativa agrícola, això implica descriure la implantació del SGSI, basat en el cicle PDCA, on es realitzarien aquests passos:

- Identificar els objectius de seguretat de la informació de la cooperativa, com ara la protecció de dades personals dels clients i empleats, i la seguretat de les operacions internes.
- Definir els processos, les polítiques i els procediments necessaris per protegir la informació sensible i assegurar la conformitat amb la legislació i els requisits normatius.
- Realitzar una avaluació de riscos per identificar les amenaces i les vulnerabilitats específiques de la cooperativa.
- Implementar controls per mitigar els riscos identificats i assegurar la protecció adequada de la informació.
- Realitzar revisions periòdiques del SGSI i implementar millores contínuament.

D'altra banda, l'ISO/IEC 27002 proporciona un conjunt de directrius i bones pràctiques per a la implementació de controls de seguretat de la informació, abordant aspectes com la gestió de riscos, la seguretat dels actius, el control d'accés i la seguretat de la comunicació, entre d'altres. Per a la cooperativa agrícola, aquesta aplicabilitat inclouria:

- Implementar els controls de l'Annex A de la ISO 27001 per garantir la seguretat de les operacions internes de l'empresa, com ara el control d'accés als sistemes informàtics, la monitorització de l'activitat de l'usuari o la implementació de polítiques de gestió de contrasenyes i controls d'accés basats en rols

En resum, aquestes normes proporcionen un marc sòlid per garantir la seguretat de la informació en una organització i ajudar a protegir-la contra amenaces internes i externes.
Cal destacar que, tot i que l'empresa ha realitzat alguns processos de millora que s'han alineat amb els requisits de la norma ISO/IEC 27001, aquests no estan integrats en un Pla Director de Seguretat específic. En aquest sentit, és crucial recopilar tots aquests esforços previs per unificar-los i integrar-los en el Pla Director de Seguretat proposat. Aquesta unificació permetrà a l'empresa

disposar d'una estratègia global i coherent per a la gestió de la seguretat de la informació, assegurant una millor alineació amb les pràctiques estàndard i una millora de la seva postura de seguretat en general.

Les versions ISO utilitzades en aquest treball són les 2023. La decisió es basa en la seva oferta d'actualitzacions més recents en matèria de seguretat de la informació. En haver de plantejar de forma inicial un SGSI a la cooperativa, el tret d'usar les més recents fa que s'incorpori un enfocament més fort en la gestió de riscos i conservi una major perseverança.

Finalment, cal mencionar que, per a la valoració dels riscos, s'utilitzarà la Metodologia d'Anàlisis y Gestió de Riscs dels Sistemes d'Informació MAGERIT. Aquesta metodologia proporciona un marc estructurat per identificar, analitzar i gestionar els riscos de seguretat associats als sistemes d'informació i permetrà avaluar completament els riscos de seguretat de la informació a la cooperativa agrícola d'arròs i identificar les mesures de seguretat més adequades per protegir la seva informació i garantir la conformitat amb els estàndards internacionals de seguretat.

## 1.4 Planificació del Treball

La planificació del treball s'estableix mitjançant un diagrama de Gantt que mostra 6 fases del projecte. En cadascuna d'aquestes, el seu final marca l'inici de la següent, tot i que s'atendrà especialment a la revisió i correcció de tots els aspectes pendents de les fases anteriors abans de continuar. Aquesta metodologia assegura una progressió ordenada i una millora contínua al llarg del desenvolupament del projecte.

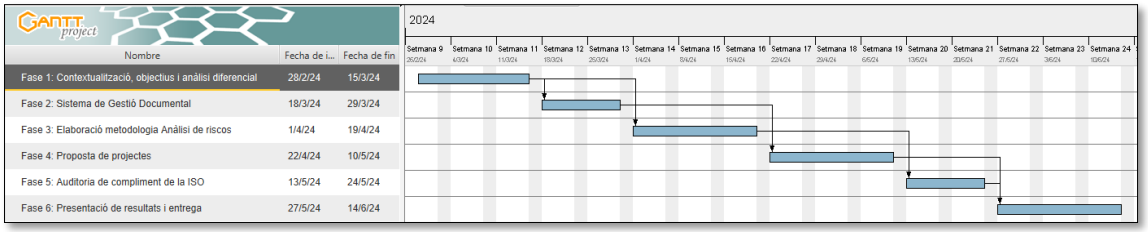


Figura 2. Diagrama de Gantt

**Fase 1: Contextualització, objectius i anàlisi diferencial:** En aquesta primera fase es coneixen les eines bàsiques que ens permeten portar a terme

el projecte. Així com el context sobre el qual es realitza, i sobre l'elecció de l'organització, es defineix l'abast, els objectius del Pla Director de Seguretat i és realitzarà un anàlisi diferencial en relació a la ISO/IEC 27001 i ISO/IEC 27002.

- Una descripció detallada de la organització.
- L'abast del pla director de Seguretat (PDS).
- L'anàlisi de compliment inicial.

**Fase 2: Sistema de Gestió Documental**: L'objectiu d'aquesta fase és la elaboració de la Política de Seguretat. Declaració de l'aplicabilitat i documentació del SGSI. Obtenint els següents documents:

- Política de seguretat.
- Procediment d'auditories internes.
- Gestió d'indicadors.
- Procediment de revisió per direcció.
- Gestió de rols i responsabilitats.
- Metodologia d'anàlisi de riscos.
- Declaració d'aplicabilitat.

**Fase 3: Estat del risc, Identificació i valoració:** En aquesta fase es busca fer una identificació i valoració dels actius i amenaces a la que està sotmesa l'organització. El resultat obtingut seria la següent documentació:

- Anàlisi detallat dels actius rellevant a nivell de seguretat de l'empresa.
- Estudi de les possibles amenaces dels sistemes de informació, així com l'impacte d'aquestes.
- Avaluació de l'impacte potencial que tindria la materialització de les diferents amenaces a les que estan exposats els nostres actius.

**Fase 4: Propostes de Projectes:** En aquesta fase es pretén fer una avaluació de tots els projectes detectats en fases anteriors i que s'hauran d'implementar per alinear-se amb els objectius del PDS, fent una quantificació econòmica i temporal.

**Fase 5: Auditoria de compliment de la ISO:** En aquesta fase es generarà un informe d'auditoria de compliment de la ISO/IEC 27001.

**Fase 6: Presentació de resultats i lliurament:** Finalment, la fase final consta de la consolidació dels resultats obtinguts, l'elaboració d'informes finals i la presentació executiva a la direcció.

### 1.5 Breu sumari de productes obtinguts

En la finalització del treball s'obtindrà una conclusió sobre l'aprofundiment de l'estat en què es trobava inicialment l'organització respecte a l'estat en què es quedarà sobre la seguretat de la informació. A més, es presentaran aquests documents finals:

- Informe de l'Anàlisi Diferencia
- Esquema Documental ISO/IEC 27001
- Anàlisi de Riscos
- Pla de projectes
- Auditoria de Compliment
- Presentació de resultats

### 1.6 Breu descripció dels altres capítols de la memòria

Explicació dels continguts de cada capítol i la seva relació amb el projecte global.

- Capítol 1. Introducció: El context, els objectius i l'enfocament del treball.
- Capítol 2. Context de l'entorn organitzatiu i de seguretat: Es descriu tota l'organització del treball, es marca l'abast del PDS i l'anàlisi diferencial.
- Capítol 3. Sistema de Gestió documental: Es farà una descripció de la documentació, les anàlisis i procediments necessaris que s'han d'incloure en el treball i que es trobaran en cas que sigui als annexos.
- Capítol 4. Anàlisi de riscos: Es farà una anàlisi detallada dels actius, l'estudi d'amenaces i una avaluació de l'impacte.
- Capítol 5. Pla de projectes: Es presenten els projectes derivats de l'anàlisi de riscos fets en el capítol anterior per millorar l'estat de la seguretat.
- Capítol 6. Auditoria de compliment: Es generarà un informe complet on es recolliran les no conformitats i observacions.
- Capítol 7. Conclusions extretes del present treball: Es generarà la documentació final.
- Capítol 8. Glossari.
- Capítol 9. Bibliografia/Webgrafia.
- Capítol 10. Annexos.

# 2. Context de l’entorn organitzatiu i seguretat

## 2.1 Descripció detallada de l’organització

L’empresa protagonista d’aquest TFM és una cooperativa agrícola d’arròs que reuneix a més de 2.500 socis dedicats a cultivar, elaborar i comercialitzar arròs amb denominació d’origen territorial. Va ser fundada fa cinquanta anys, i s’ha mantingut fidel als seus valors centrals de qualitat, sostenibilitat i compromís amb la comunitat agrícola local. L’eix principal està format per un total de 60 treballadors i l’empresa cada cop facilita més la seva expansió i el seu reconeixement tant nacionalment com internacionalment.

La cooperativa ofereix una àmplia gamma de serveis als seus socis, des de l'assessorament tècnic per a millorar els rendiments dels cultius fins a la comercialització i distribució de l'arròs i verdura amb denominació d'origen territorial. A més, l’organització s'ha destacat per la seva inversió en tecnologia i innovació, implementant pràctiques agrícoles sostenibles i adoptant noves tecnologies per millorar l'eficiència i la qualitat dels seus productes.

La presència de la cooperativa no només es limita al mercat local, sinó que també ha estat capaç de guanyar reconeixement a escala nacional i internacional. Mitjançant la seva participació en fires i esdeveniments sectorials, així com a través de la distribució d'arròs de qualitat en mercats europeus i internacionals, la cooperativa ha consolidat la seva posició amb un renom important en la regió.

Tot i que tradicionalment l'agricultura ha estat vista com una indústria aïllada de les tecnologies de la informació, en els últims anys s'ha produït una creixent digitalització del sector, i la cooperativa, com s’ha dit prèviament, està adoptant noves tecnologies per millorar la gestió de les explotacions, el monitoratge dels cultius i la comercialització dels seus productes.  Això inclou l'ús de sistemes de gestió de la cadena d'aprovisionament, plataformes de comerç electrònic per a la venda de productes en línia i solucions de comunicació interna per facilitar la col·laboració entre els diferents equips i departaments.

El sector agrícola s'enfronta a una creixent amenaça de ciberatacs, tal com es demostra en estudis recents que mostren un augment del nombre d'atacs cibernètics, la cooperativa està exposada a diversos riscos i amenaces en línia.

Entre aquests, es troben els possibles ciberatacs dirigits a la seva infraestructura tecnològica, com ara atacs de denegació de servei (DDoS), intents de phishing per obtenir dades confidencials dels empleats o clients, i altres formes de ciberdelinqüència com l'ús maliciós de malware.

A través d'una carta de serveis, la cooperativa proporciona informació essencial sobre els seus serveis, els termes i condicions associats, i els mecanismes per a la comunicació i la resolució de reclamacions.

**La carta de serveis de la cooperativa agrícola inclou:**

- Informació general i legal sobre l'organització: Descripció de la missió, visió i valors de l'empresa, així com informació sobre la seva estructura organitzativa i les seves responsabilitats legals.

- Compromisos de qualitat: Enumeració dels estàndards de qualitat que s'ha compromès a mantenir en la seva relació amb els socis i clients.

- Indicadors de compliment: Presentació dels indicadors que mesuren el compliment dels compromisos de qualitat establerts.

- Mesures d'esmena i compensació: Detall de les accions que l'empresa prendrà en cas d'incompliment dels seus compromisos de qualitat, incloent-hi possibles mesures de compensació per als socis i clients afectats.

- Mecanismes de comunicació: Descripció dels canals de comunicació disponibles per als socis i clients per presentar queixes, reclamacions o suggeriments.

- Informació complementària: Altres detalls rellevants com ara horaris d'atenció, polítiques de privacitat i drets dels consumidors.

Aquesta carta de serveis aporta valor a l'empresa al millorar la transparència i la confiança, augmentar la satisfacció dels clients, gestionar eficaçment les reclamacions i diferenciar-se de la competència. Això contribueix a la imatge i al rendiment general de l'empresa en el seu mercat.

En l'àmbit d'organització, la cooperativa opera amb una estructura jeràrquica clara i funcional. La direcció general o junta directiva, integrada per membres destacats de la comunitat agrícola i empresarial, exerceix un paper clau en la presa de decisions estratègiques i l'orientació de l'empresa. A més, l'organització compta amb tres grans departaments funcionals, que són: gestió i

administració, producció i operacions, i negoci i mercat. Els departaments juntament amb les seves àrees treballen de manera coordinada per assegurar el bon funcionament de les operacions diàries.

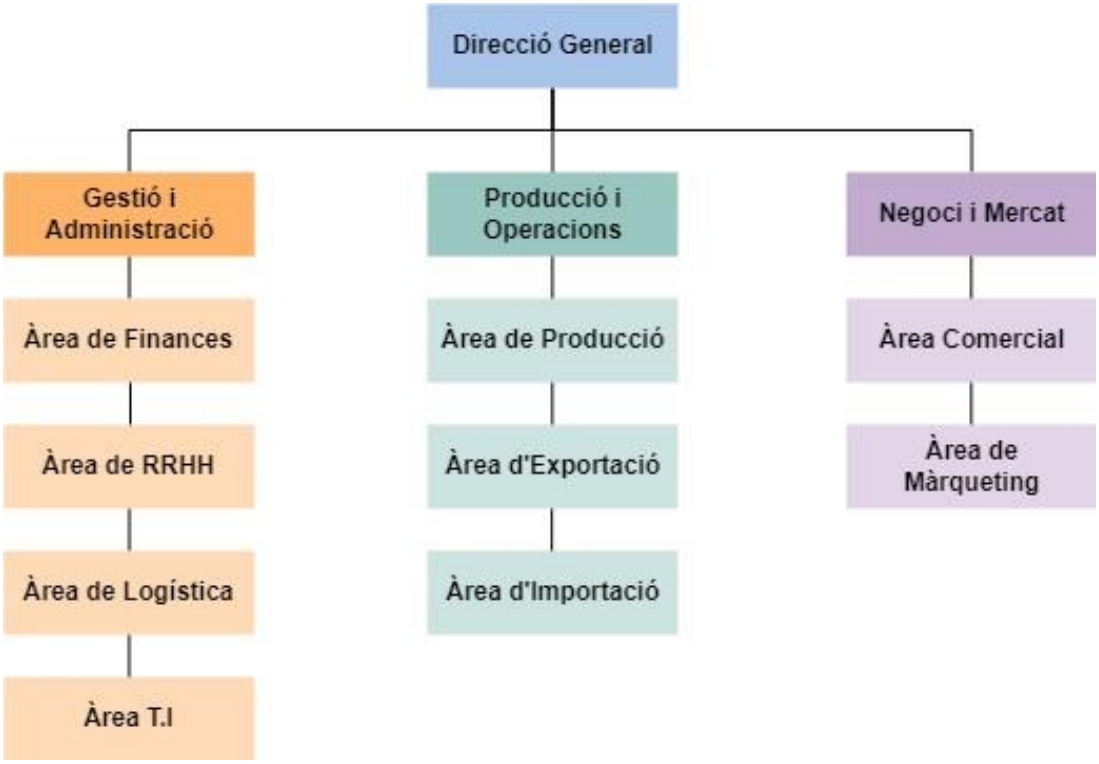


Figura 3. Organigrama de l'empresa

Fins ara, la responsabilitat de garantir la seguretat de la informació recau principalment en l'Àrea de Tecnologies de la Informació (T.I), encarregada de gestionar els aspectes tecnològics bàsics relacionats amb la seguretat dels sistemes informàtics i la infraestructura de xarxes. No obstant això, com a part del procés d'implementació del SGSI, s'està considerant tant la creació d'un departament específic dedicat exclusivament a la gestió de la seguretat de la informació a l'empresa a través d'una formació dels treballadors existents com la subcontractació de personal tècnic especialitzat en l'àrea de seguretat en la informació. Aquest últim, formaria part d'un actor extern rellevant per al projecte.

## Inventari d’actius

A continuació, hi ha la taula d'inventari d'actius, que és una pràctica fonamental en la gestió de la seguretat de la informació de qualsevol per identificar, classificar i registrar tots els actius d'informació rellevants per a l'empresa, siguin físics o virtuals, tangibles o intangibles. Aquest procés proporciona una visió completa dels recursos d'informació de l'organització i permet una millor comprensió dels riscos i una gestió més efectiva de la seguretat.

| INVENTARI D’ACTIUS | | | |
|---|---|---|---|
| **Tipus** | **Actiu** | **Ubicació** | **Responsable** |
| **Dades (D)** | Informació dels membres | Oficina central | Gestió i administració |
| **Dades (D)** | Dades dels clients | Base de dades | Gestió i administració |
| **Dades (D)** | Informació financera | Servidors | Gestió i administració |
| **Dades (D)** | Registres nòmines | Servidor de nòmines | Gestió i administració |
| **Dades (D)** | Còpies de seguretat | Cabina d'emmagatzematge | Àrea T.I |
| **Claus criptogràfiques (KY)** | Claus d’encriptació portàtils | Custòdia segura | Seguretat |
| **Serveis (S)** | VPN | Xarxa interna | Àrea T.I |
| **Serveis (S)** | Directori Actiu | Servidors | Àrea T.I |
| **Serveis (S)** | Web | Servidor web | Àrea T.I |
| **Serveis (S)** | Correu O365 | Núvol | Àrea T.I |
| **Hardware (HW)** | Servidors | Sala de servidors | Àrea T.I |
| **Hardware (HW)** | Portàtils | Oficina central | Departaments i Àrea T.I |
| **Hardware (HW)** | Telèfons mòbils | Personal | Departament i Àrea T.I |
| **I Hardware (HW)** | Impressores | Diverses ubicacions | Departaments i Àrea T.I |
| **Hardware (HW)** | Escàners | Diverses ubicacions | Departaments i Àrea T.I |
| **Aplicacions informàtiques (SW)** | SAP | Servidors | Departaments i Àrea T.I |
| **Aplicacions informàtiques (SW)** | Plataforma corporativa | Núvol | Àrea T.I |
| **Aplicacions** | Antivirus | Núvol | Seguretat |

| | | | |
|---|---|---|---|
| **informàtiques (SW)** | | | |
| **Aplicacions informàtiques (SW)** | Office 365 | Núvol | Àrea T.I |
| **Suports d'informació (MED)** | Cabina d'emmagatzematge (discs durs i USB) | Instal·lacions | Àrea T.I |
| **Equipament auxiliar (AUX)** | SAI | Instal·lacions | Manteniment |
| **Equipament auxiliar (AUX)** | Equips de climatització | Instal·lacions | Manteniment |
| **Equipament auxiliar (AUX)** | Càmeres de seguretat | Instal·lacions | Seguretat |
| **Xarxes de comunicació (COM)** | Xarxa pública | Instal·lacions | Àrea T.I |
| **Xarxes de comunicació (COM)** | Xarxa privada | Instal·lacions | Àrea T.I |
| **Xarxes de comunicació (COM)** | Xarxa telefònica | Instal·lacions | Àrea T.I |
| **Instal·lacions (L)** | Planta de processament | Instal·lacions | Direcció general i Producció |
| **Instal·lacions (L)** | Seu central | Instal·lacions | Direcció general i Administració |
| **Instal·lacions (L)** | Oficina territorial | Instal·lacions | Direcció general i Administració |
| **Persones (P)** | Treballadors | Personal | Recursos Humans |
| **Persones (P)** | Administradors | Personal | Gestió i administració |
| **Persones (P)** | Proveïdors | Tercers | Compres |
| **Persones (P)** | Clients | Extern | Vendes |

## Mapatge dels rols necessaris en el SGSI

| Rols | Possibles càrrecs |
|---|---|
| Responsable de Seguretat de la Informació (CISO) | Director General o Cap de l'àrea T.I |
| Coordinador de Resposta a Incidents Cibernètics | Cap de l'àrea T.I o especialista en seguretat informàtica |
| Responsable de Legalitat, Política i Conformitat Cibernètica | Servei subcontractat + Direcció General |
| Especialista en Intel·ligència de Amenaces Cibernètiques | Servei subcontractat o especialista en seguretat informàtica format de l'àrea T.I |
| Arquitecte de Ciberseguretat | Servei subcontractat o especialista en seguretat informàtica format de l'àrea T.I |
| Auditor de Ciberseguretat | Servei subcontractat |
| Educador de Ciberseguretat | Servei subcontractat o especialista en seguretat informàtica format de l'àrea T.I |
| Implementador de Ciberseguretat | Servei subcontractat |
| Investigador de Ciberseguretat | Servei subcontractat |
| Gestor de Riscos de Ciberseguretat | Pot ser assumit pel responsable de Seguretat de la informació |

Taula 1. Mapatge de rols necessaris SGSI

## Infraestructura de l'empresa:

**Seu central:** És un edifici administratiu on es realitzen les funcions directives, administratives i de gestió. Hi ha despatxos per als membres de la junta directiva, sales de reunió, departaments administratius (finances, recursos humans i logística) i departaments T.I. A més dels espais comuns com ara recepció i àrees d'espera.

**Planta de processament**: En aquest espai es realitza la neteja, l'emmagatzematge i el processament de l'arròs. Aquesta instal·lació inclou podria maquinària especialitzada per al processament de grans quantitats d'arròs, a més de magatzems així com magatzems per a l'emmagatzematge de la matèria primera i del producte acabat. D'altra banda, per al processament hi ha també elements actius connectats a la xarxa, com ara servidors de producció on les dades de ordres, registres i llistes de materials queden registrades, tot això es controla amb equips destinats per a aquest registre.

**Oficina territorial:** Aquesta oficina serveix com a punt de contacte local per als clients i proveïdors, així com per a la coordinació de les operacions regionals. Està repleta d'equips informàtics on els treballadors tenen el seu correu d'empresa, un sistema de telefonia i equipament.

El següent diagrama inclou de manera visual els següents elements: equips, servidors, maquinari, comunicacions, software i serveis al núvol.

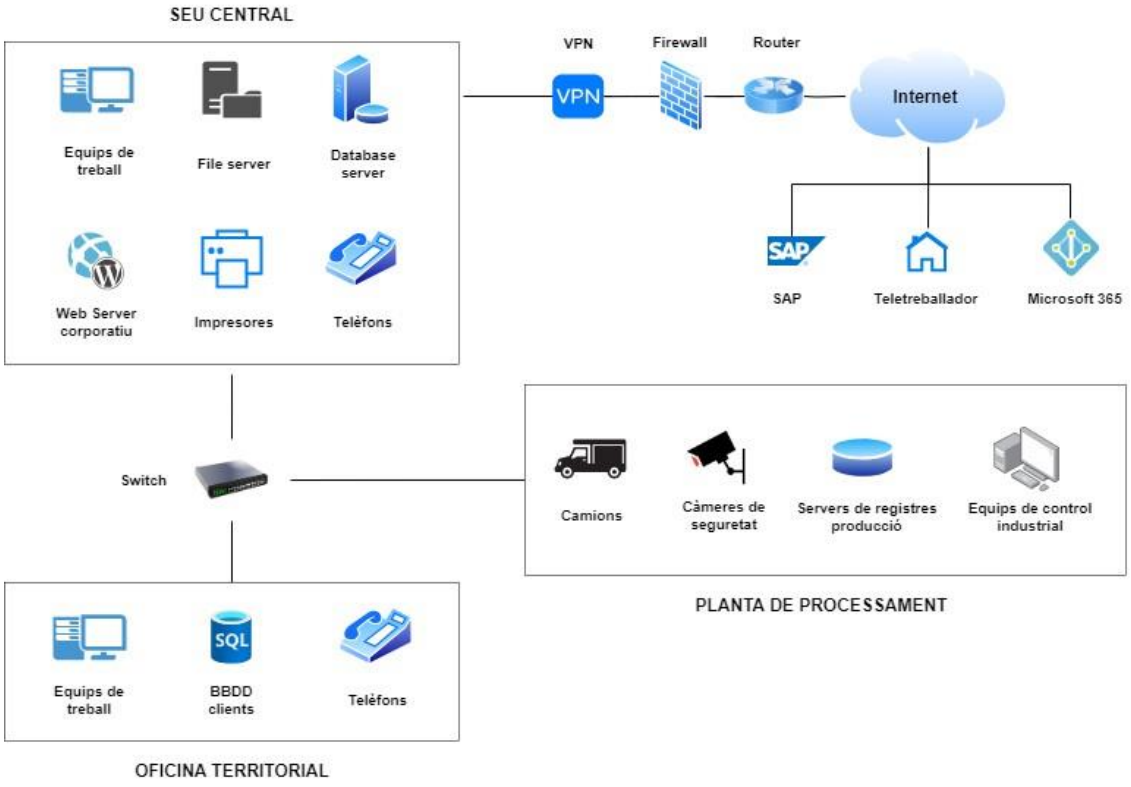


Figura 4. Diagrama d'infraestructura i arquitectura de l'empresa

## Processos dels serveis

Serveis finals:

- Procés de producció i distribució

Serveis instrumentals i de suport:

- Procés de finances
- Procés de RRHH
- Procés de logística
- Procés TIC generals
- Procés d'acció comercial
- Procés de màrqueting

A més, la cooperativa recorre a serveis externs per a completar les seves operacions:

- Gestió de seguretat física: Subcontracten una empresa especialitzada en la vigilància i el control d'accés físic a les instal·lacions.

- Manteniment: El suport tècnic per a la instal·lació, manteniment i reparació de maquinària agrícola i equips de processament també es subcontractat.

Tots els processos esmentats anteriorment impliquen la gestió de la informació que pot ser sensible i ha de ser protegida per garantir la seguretat de la informació de l'organització:

**Procés de producció i distribució**

- **Enfocament SGSI:** És vital per al SGSI, perquè implica la gestió de la informació relacionada amb la producció de l'arròs i la seva distribució, com ara sobre els processos de producció, inventari, logística i distribució.
- **Actors involucrats:** Personal de l'àrea de producció, exportació i importació.
- **Flux de dades:** Informació sobre la producció d'arròs, inventari de productes acabats, rutes de distribució, dades de clients i comandes.

**Procés de finances**:

- **Enfocament SGSI** Impliquen informació crítica sobre finances, pagaments i facturació que ha de ser protegida.
- **Actors involucrats:** Personal de l'àrea de finances.
- **Flux de dades:** Transaccions financeres, informes comptables, nòmines dels empleats, facturació i pagaments als proveïdors.

**Procés de RRHH**

- **Enfocament SGSI:** Implica la gestió de la informació personal dels treballadors, com ara dades personals, contractes laborals, històrics salarials, etc., que també s'han de protegir adequadament.
- **Actors involucrats:** Personal de l'àrea de RRHH.
- **Flux de dades:** Dades dels empleats, contractes laborals, registre d'assistència, sol·licituds de permisos o vacances.

**Procés de logística:**

- **Enfocament SGSI:** La informació sobre inventari, trasllats de mercaderies, proves de qualitat és crítica per al SGSI i pot implicar riscos per a la seguretat de la informació si no es gestiona adequadament.
- **Actors involucrats:** Personal de l'àrea de logística.
- **Flux de dades:** Planificació de rutes de transport, control d'inventari, seguiment de lliuraments, gestió de devolucions.

**Procés TIC generals**

- **Enfocament SGSI:** També és essencial, inclou la gestió de la infraestructura tecnològica de l'empresa (seguretat de les xarxes, sistemes, dades, etc.).
- **Actors involucrats:** Personal de l'àrea I.T
- **Flux de dades:** Manteniment dels sistemes informàtics, gestió de xarxes, seguretat informàtica, suport tècnic als usuaris.

**Procés d'acció comercial**

- **Enfocament SGSI:** La informació comercial també pot ser sensible i ha de ser protegida per assegurar la seguretat de la informació de l'empresa.
- **Actors involucrats:** Personal de l'àrea comercial.
- **Flux de dades:** Seguiment de clients potencials, gestió de contactes, ofertes comercials, registre de vendes.

**Procés d'acció màrqueting**

- **Enfocament SGSI:** La informació de màrqueting també pot ser sensible i ha de ser protegida per assegurar la seguretat de la informació de l'empresa.
- **Actors involucrats:** Personal de l'àrea de màrqueting.
- **Flux de dades:** Creació de campanyes publicitàries, anàlisi de mercat, gestió de xarxes socials, informes de rendiment de campanyes.

**Serveis externs subcontractats**

- **Gestió de seguretat física:** Personal de seguretat subcontractat que assegura que es realitzin inspeccions i proves regulars per la seguretat continuada de les instal·lacions. Així com supervisar el monitoratge CCTV per qualsevol incidència poder respondre ràpidament amb l'organització.
- **Manteniment:** Tècnics subcontractats per a la reparació i el manteniment de maquinària agrícola i equips de processament.

A continuació, es mostra l'esquema dels diversos processos comentats prèviament que fan possible que es desenvolupin els serveis. Aquest, mostra també les seves dependències: Els processos en blau (de producció i distribució) estan relacionats amb els de suport (els grocs) així com en client.

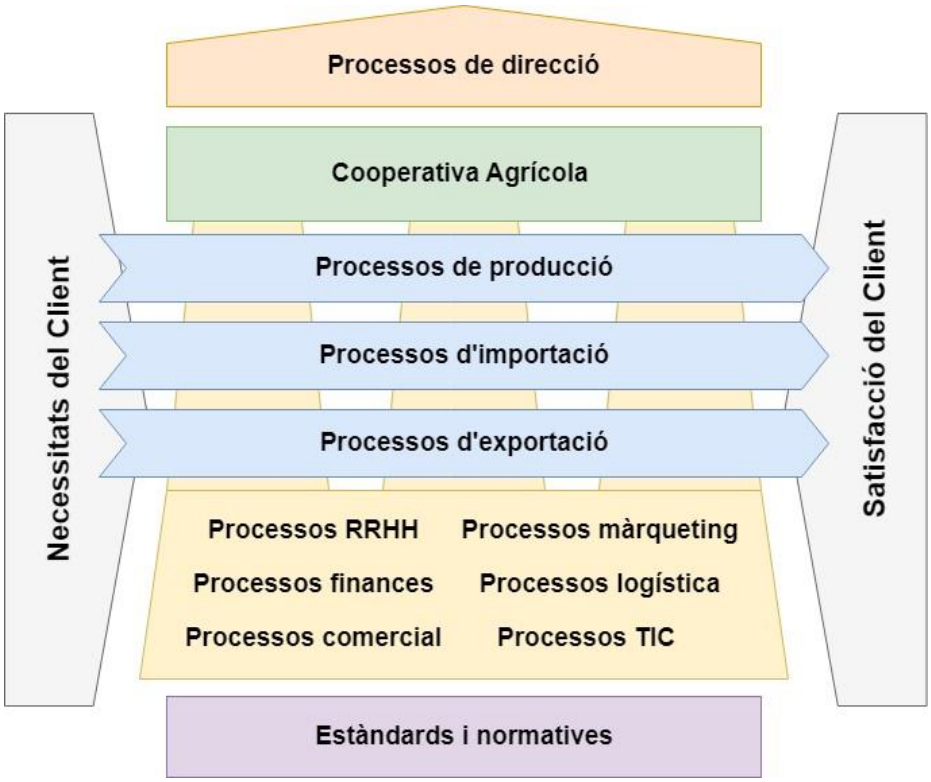

Figura 5. Mapa de Procesos

**Anàlisi DAFO**

S'ha dut a terme una anàlisi de l'organització mitjançant l'ús de l'anàlisi DAFO, una eina que proporciona una visió integral del seu entorn de negoci i la seva capacitat estratègica. Aquesta, s'enfoca en identificar les fortaleses i debilitats internes de l'empresa, així com a explorar les amenaces i oportunitats presents en el seu context extern. A través d'aquesta metodologia, es busca obtenir una comprensió completa dels factors clau que influeixen en el rendiment i la direcció estratègica de l'organització.

| | Punts forts | Punts dèbils |
|---|---|---|
| **Origen Intern** | **DEBILITATS**<br><br>- La cooperativa actualment no té implementat un SGSI, la qual cosa pot exposar les dades sensibles dels clients i comprometre la seguretat de la informació.<br><br>- Manca de formació en seguretat de la informació: El personal no està adequadament format en qüestions de seguretat de la informació, augmentant el risc d'errors i violacions de la seguretat.<br><br>- Dependència excessiva de sistemes informàtics antiquats: que pot limitar la capacitat de la cooperativa per implementar mesures de seguretat modernes i eficaces. | **FORTALESES**<br><br>- La cooperativa gaudeix d'una reputació consolidada com a líder en el sector agrícola, amb una base sòlida de clients i socis.<br><br>- La cooperativa disposa de recursos financers suficients per implementar un SGSI i altres mesures de seguretat de la informació.<br><br>- La cooperativa compta amb el suport de la comunitat agrícola local, la qual cosa pot facilitar la implementació de noves iniciatives i mesures de millora. |
| **Origen extern** | **AMENACES**<br><br>- L'increment de les amenaces cibernètiques pot posar en perill la seguretat de les dades de la cooperativa, especialment si no s'implementen mesures de protecció adequades.<br><br>- Canvis en la legislació de protecció de dades poden requerir que la cooperativa faci ajustos significatius per complir amb els nous requisits, augmentant la càrrega administrativa i els costos associats.<br><br>- La competència en el sector agrícola pot obligar la cooperativa a mantenir-se al dia amb les millors pràctiques i innovacions tecnològiques en matèria de seguretat de la informació per mantenir la seva posició de lideratge. | **OPORTUNITATS**<br><br>- Implementar un SGSI pot millorar la confiança dels clients en la cooperativa, demostrant el seu compromís amb la protecció de les seves dades i la seva seguretat.<br><br>- L'èxit en la implementació de mesures de seguretat de la informació pot obrir noves oportunitats de creixement i expansió per a la cooperativa, ja que pot millorar la seva competitivitat i atracció per als clients i socis.<br><br>- L'adopció de sistemes informàtics més segurs pot millorar la eficiència operativa de la cooperativa, reduint els riscos de temps d'inactivitat i pèrdua de dades. |

Figura 6. Anàlisi DAFO

## 2.2 Anàlisi Diferencial

Abans de començar amb el projecte d'implantació, es farà una anàlisi diferencial de les mesures de seguretat i la normativa que tingui l'organització amb relació a la seguretat de la informació. Aquesta anàlisi diferencial s'efectuarà respecte a les normatives ISO/IEC 27001:2023 i ISO/IEC 27002:2023, i ens permetrà conèixer de manera global l'estat actual de l'organització en relació amb la seguretat de la informació.

L'objectiu de l'anàlisi és la verificació de la implantació, en relació amb els processos detectats al PDS, dels controls establerts a la norma. Com a resultat, es proposen una sèrie de recomanacions per la qual la seva implantació és necessària per millorar la seguretat de la informació, així com per prioritzar l'assignació de recursos sobre les àrees amb més criticitat i optimitzar els costos/beneficis.

Aquesta valoració es farà segons aquesta taula basada en el nivell de maduresa dels controls d'acord al Model de Maduresa de Capacitat (CMM).

| Efectivitat | CMM | Valor | Significat | Descripció |
|---|---|---|---|---|
| 0% | L0 | 0 | Inexistent | Carència completa de qualsevol procés que reconeguem.<br>No s'ha reconegut que existeixi cap problema a resoldre. |
| 10% | L1 | 1 | Inicial / Ad-hoc | Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal.<br>Els procediments son inexistents o localitzats en àrees concretes.<br>No existeixen plantilles definides a nivell corporatiu |
| 50% | L2 | 2 | Reproduïble, però intuïtiu | Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca.<br>E ha s normalitzen les "bones practiques" en base a l'experiència i al mètode.<br>No hi ha comunicació o entrenament formal, les responsabilitats queden a càrrec de cada individu.<br>Es depèn del grau de coneixement de cada individu. |
| 90% | L3 | 3 | Procés definit | La organització sencera participa al procés.<br>Els processos estan implantats, documentats i comunicats mitjançant entrenament. |
| 95% | L4 | 4 | Gestionat i mesurable | Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos.<br>Es disposa de tecnologia per automatitzar el flux de treball, s'ha de tenir eines per a millorar la qualitat i la eficiència. |
| 100% | L5 | 5 | Optimitzat | Els processos estan sota constant millora.<br>En base criteris quantitatius es determinen les desviacions més comunes i s'optimitzen els processos. |

Taula 2. Model de maduresa dels controls (CMM)

A continuació, es detallarà l'anàlisi diferencial ISO/IEC 27001:2023. Aquest es basa en veure i valorar el nivell de compliment actual de la normativa corresponent. D'acord amb els resultats obtinguts, es poden identificar els aspectes que més esforços s'han de centrar per aconseguir una correcta implementació del SGSI.

| Secció | Requisit ISO/IEC 27001 | Valor | Justificació |
|---|---|---|---|
| **4** | **Context de l'organització** | **1,75** | |
| **4,1** | **Context organitzacional** | | |
| 4,1 | Determinar els objectius de l'SGSI de l'organització i qualsevol qüestió que en pugui comprometre l'efectivitat | 2 | La cooperativa té els seus procediments de seguretat, però no es té cap política detallada i aprovada per l'organització que defineixi l'abast i els objectius a nivell institucional. |
| **4,2** | **Comprensió partes interessades** | | |
| 4.2 (a) | Identificar les parts interessades incloent-hi lleis aplicables, regulacions, contractes, etc. | 3 | S'han identificat algunes parts interessades, però encara hi ha mancances en la identificació de les lleis aplicables i les regulacions rellevants. |
| 4.2 (b) | Determinar els requisits rellevants respecte a la seguretat de la informació i les obligacions. | 3 | S'han definit alguns requisits rellevants, però encara s'han de determinar completament les obligacions legals i normatives aplicables. |
| **4,3** | **Abast del SGSI** | | |
| 4,3 | Determinar y documentar l'abast del SGSI | 1 | L'abast del SGSI s'ha començat a definir, però encara no està completament documentat. |
| **4,4** | **SGSI** | | |
| 4,4 | Establir, implementar, mantenir i millorar contínuament un SGSI de conformitat amb la norma | 1 | Encara no s'ha establert ni implementat un SGSI a la cooperativa. Es necessita un treball continu per aconseguir la conformitat amb la norma ISO/IEC 27001. |
| **5** | **Lideratge** | **1,66** | |
| **5,1** | **Lideratge i compromís** | | |
| 5,1 | La alta direcció ha de demostrar lideratge & compromís en relació con el SGSI. | 2 | Hi ha un compromís declarat per part de la direcció, però encara es necessita un lideratge més actiu i visible en la implementació del SGSI. |
| **5,2** | **Política** | | |
| 5,2 | Establir la política de seguretat de la informació | 1 | No s'ha establert una política de seguretat de la informació. És necessari que la direcció prioritzi aquesta tasca. |
| **5,3** | **Rols, responsabilitats i autoritats en la organització** | | |
| 5,3 | Assignar y comunicar els rols i les responsabilitats de la seguretat de la informació. | 2 | S'han començat a definir alguns rols i responsabilitats en matèria de seguretat de la informació (equip I.T), però encara no |

| | | | |
|---|---|---|---|
| | | | s'ha efectuat com a un equip independent. Es necessita un esforç addicional per assegurar que tothom entengui els seus rols i responsabilitats. |
| **6** | **Planificació** | **1,77** | |
| **6,1** | **Accions per tractar amb els riscos i oportunitats** | | |
| 6.1.1 | Dissenyar / planificar el SGSI per satisfer els requisits, tractant amb els riscos & oportunitats | 2 | S'ha començat a dissenyar de manera inicial un SGSI per satisfer els requisits, però encara no s'han tractat tots els riscos i oportunitats de manera completa i efectiva. |
| 6.1.2 | Definir i aplicar un procés d'apreciació de riscs de seguretat de la informació. Documentar i aplicar un procés de tractament de riscos de seguretat de la informació | 1 | Encara no s'ha definit ni aplicat un procés d'apreciació de riscos ni un procés de tractament de riscos de seguretat de la informació. |
| 6.1.3 | Documentar i aplicar un procés de tractament de riscos de seguretat de la informació | 1 | No s'ha documentat ni aplicat un procés de tractament de riscos de seguretat de la informació. |
| **6,2** | **Objectius i plans de seguretat de la informació** | | |
| 6,2 | Establir i documentar els objectius i els plans de seguretat de la informació | 2 | Els objectius i plans de seguretat de la informació s'han documentat i està en fase de realització d'un anàlisis de risc, en el què s'avaluïn tots els actius implicats en el tractament de la informació, i l'establiment d'un pla pel tractament del risc. |
| **6,3** | **Planificació de canvis** | | |
| 6,3 | Els canvis substancials a l'SGSI s'han de dur a terme de manera planificada | 2 | S'ha reconegut la importància de dur a terme canvis substancials de manera planificada, però encara cal desenvolupar un procés formal per a això. |
| **7** | **Suport** | **2,26** | |
| **7,1** | **Recursos** | | |
| 7,1 | Determinar i proporcionar els recursos necessaris per al SGSI | 2 | S'han començat a determinar i proporcionar els recursos necessaris per al SGSI, però encara es necessita un esforç addicional per garantir que tots els recursos requerits estiguin disponibles i s'utilitzin eficaçment. |
| **7,2** | **Competències** | | |
| 7,2 | Determinar, documentar i posar a disposició les competències necessàries | 3 | La cooperativa s'assegura que hi hagi formacions a tot el personal per evitar que siguin incompetents en el seu càrrec. Inclosos els de l'àrea I.T. |
| **7,3** | **Conscienciació** | | |
| 7,3 | Establir un programa de conscienciació en seguretat | 3 | S'han realitzat diverses accions formatives sobre la seguretat de la informació, proposades per l'àrea I.T i guiades per aquests. |
| **7,4** | **Comunicació** | | |
| 7,4 | Determinar la necessitat per a les comunicacions internes i externes | 2 | El personal i la junta reconeix la importància de determinar les necessitats de |

| | | | |
|---|---|---|---|
| | rellevants a l'SGSI | | comunicació internes i externes rellevants per a l'SGSI. No obstant això, encara s'ha de desenvolupar un pla concret. |
| **7,5** | **Informació documentada** | | |
| 7.5.1 | Proveir la documentació requerida per la norma així com la requerida per l'organització | 2 | S'ha començat a proveir la documentació requerida per la norma i per l'organització, però encara cal completar aquest procés per garantir que tota la documentació necessària estigui disponible. |
| 7.5.2 | Proveir títols, autors, etc per a la documentació, adequar el format consistentment, revisar-los i aprovar-los | 1 | No es produeix per ara aquesta tasca, però es té en compte i és crucial per garantir la coherència i la integritat de la documentació. |
| 7.5.3 | Controlar la documentació adequadament | 1 | Per ara no s'ha implementat un sistema adequat per controlar la documentació. És necessari establir un procés per garantir que tota la documentació estigui controlada i mantinguda actualitzada de manera eficaç. |
| **8** | **Operació** | **1** | |
| **8,1** | **Planificació i control operacional** | | |
| 8,1 | Planificar, implementar, controlar i documentar el procés de l'SGSI per gestionar els riscos (ex. un pla de tractament de riscos) | 1 | Encara no s'ha planificat, implementat ni documentat adequadament el procés de l'SGSI per gestionar els riscos. Està pendent de realitzar. |
| **8,2** | **Apreciació del risc de seguretat de la informació** | | |
| 8,2 | (Re)fer l'apreciació i documentar els riscos de seguretat de la informació en forma regular & davant de canvis o modificacions | 1 | Encara no s'ha realitzat una apreciació completa dels riscos de seguretat de la informació, ni s'ha documentat adequadament. Està pendent de realitzar. |
| **8,3** | **Tractament del risc de seguretat de la informació** | | |
| 8,3 | Implementar el pla de tractament de riscos (tractar els riscos) i documentar-ne els resultats | 1 | Encara no s'ha implementat el pla de tractament de riscos ni s'han documentat els resultats. Està pendent de realitzar. |
| **9** | **Avaluació de l'exercici** | **1** | |
| **9,1** | **Seguiment, mesura, anàlisi i avaluació** | | |
| 9,1 | Fer seguiment, mesurar, analitzar i avaluar l'SGSI i els controls | 1 | Encara no s'ha dut a terme una adequada vigilància, mesura, anàlisi i avaluació de l'SGSI i els seus controls. Està pendent de realitzar. |
| **9,2** | **Auditoria interna** | | |
| 9,2 | Planificar i dur a terme auditories internes de l'SGSI | 1 | Encara no s'han planificat ni dut a terme auditories internes de l'SGSI. Està pendent de realitzar. |
| **9,3** | **Revisió per la direcció** | | |
| 9,3 | Emprendre revisions per la direcció del SGSI regularment | 1 | Encara no s'han realitzat revisions per la direcció del SGSI regularment. Està pendent de realitzar. |
| **10** | **Millora** | **1** | |

| | | | |
|---|---|---|---|
| **10,1** | **Millora continua** | | |
| 10,1 | Millorar contínuament el SGSI | 1 | Està pendent de realitzar perquè encara no s'ha implementat el SGSI, però son conscients que ha de fer-se. |
| **10,2** | **No conformitat i accions correctives** | | |
| 10,2 | Identificar, corregir i dur a terme accions per prevenir la recurrència de no-conformitats, documentant les accions | 1 | Està pendent de realitzar, però serà una tasca a tenir en compte quan es realitzi el SGSI. |

Taula 3. Anàlisi de compliment inicial ISO 27001:2033

### Interpretació dels resultats GAP 27001:

Després d'analitzar l'estructura i les pràctiques de seguretat de la cooperativa, queda a la vista que encara hi ha àrees importants que requereixen millora per aconseguir la conformitat amb la norma ISO/IEC 27001. Tot i que l'empresa ha pres alguns passos en la direcció correcta, com ara la identificació de parts interessades i la conscienciació sobre seguretat de la informació, encara hi ha mancances significatives.

Per la qual cosa, es designarà un equip que lideri i implementi tot el SGSI. Aquest equip serà independent al de l'àrea I.T, i serà l'encarregat de fer el pla de seguretat que permeti consolidar la confidencialitat, integritat i disponibilitat. Com es pot veure en aquesta figura, l'estat d'implementació inicial està en un estat de maduresa prou baix, perquè encara fa falta definir molts aspectes i els objectius encara queden lluny.

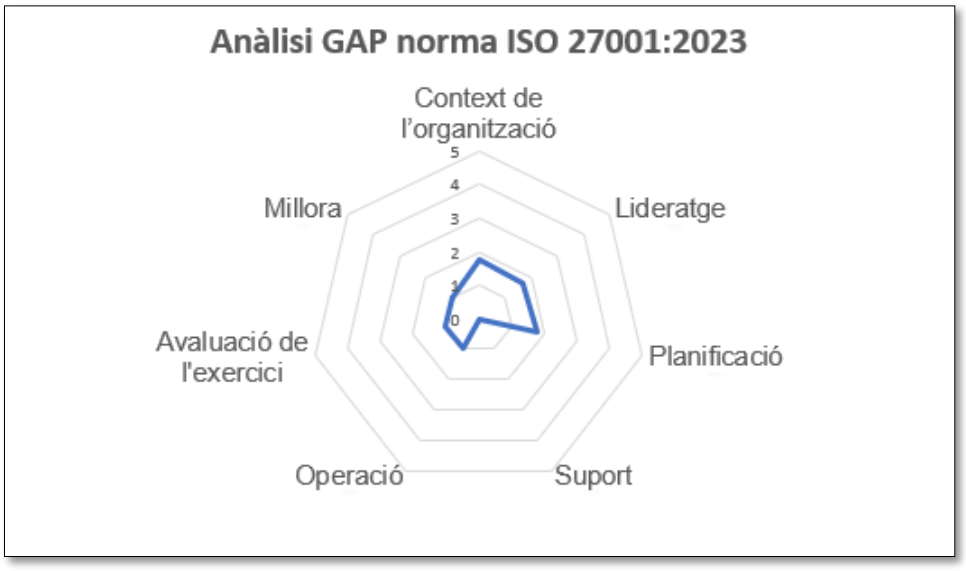


Figura 7. Resultats del anàlisi GAP norma ISO 27001

**Context de l'organització (Valor: 1,75):** És necessari establir una política de seguretat de la informació detallada i aprovada per l'organització per definir clarament els objectius i l'abast de l'SGSI.

**Lideratge (Valor: 1,66):** Malgrat l'existència d'un compromís declarat per part de la direcció, cal un lideratge més actiu i visible en la implementació del SGSI, així com l'establiment d'una política de seguretat de la informació.

**Planificació (Valor: 1,77):** És essencial completar el disseny i la planificació del SGSI per abordar tots els riscos i oportunitats de manera completa i efectiva. A més, cal establir un procés formal per a la planificació de canvis substancials a l'SGSI.

**Suport (Valor: 2,26):** Tot i que s'han començat a determinar i proporcionar recursos i competències necessàries per a l'SGSI, cal un esforç addicional per garantir que tots els recursos requerits estiguin disponibles i s'utilitzin eficaçment. A més, es necessita desenvolupar un pla concret per a les comunicacions internes i externes rellevants i completar la provisió de la documentació requerida.

**Operació (Valor: 1):** Es requereix planificar, implementar i documentar adequadament el procés de l'SGSI per gestionar els riscos, així com realitzar una apreciació completa dels riscos de seguretat de la informació i implementar un pla de tractament de riscos.

**Avaluació de l'exercici (Valor: 1):** És essencial dur a terme una adequada vigilància, mesura, anàlisi i avaluació de l'SGSI i els seus controls, així com planificar i dur a terme auditories internes de l'SGSI i revisions per la direcció del SGSI regularment.

**Millora (Valor: 1):** Cal millorar contínuament el SGSI i implementar accions per identificar, corregir i prevenir la recurrència de no-conformitats.

Com a conclusió, la cooperativa actualment ha avançat un poc en diversos aspectes relacionats amb la implementació de l'SGSI, però encara hi ha feina per fer per garantir el compliment adequat de la normativa ISO/IEC 27001:2023 i la millora continua de la seguretat de la informació. Per aquesta raó, s'han de centrar els esforços en les àrees identificades i prioritzar les accions necessàries per aconseguir una implementació efectiva del SGSI.

**Interpretació dels resultats GAP 27002:**

Finalment, l'anàlisi diferencial ISO/IEC 27002:2023, aquest s'ha realitzat amb els controls de l'Annex A de la ISO 27001:2023. Com podem veure, el nivell de compliment actual dels controls és el següent:

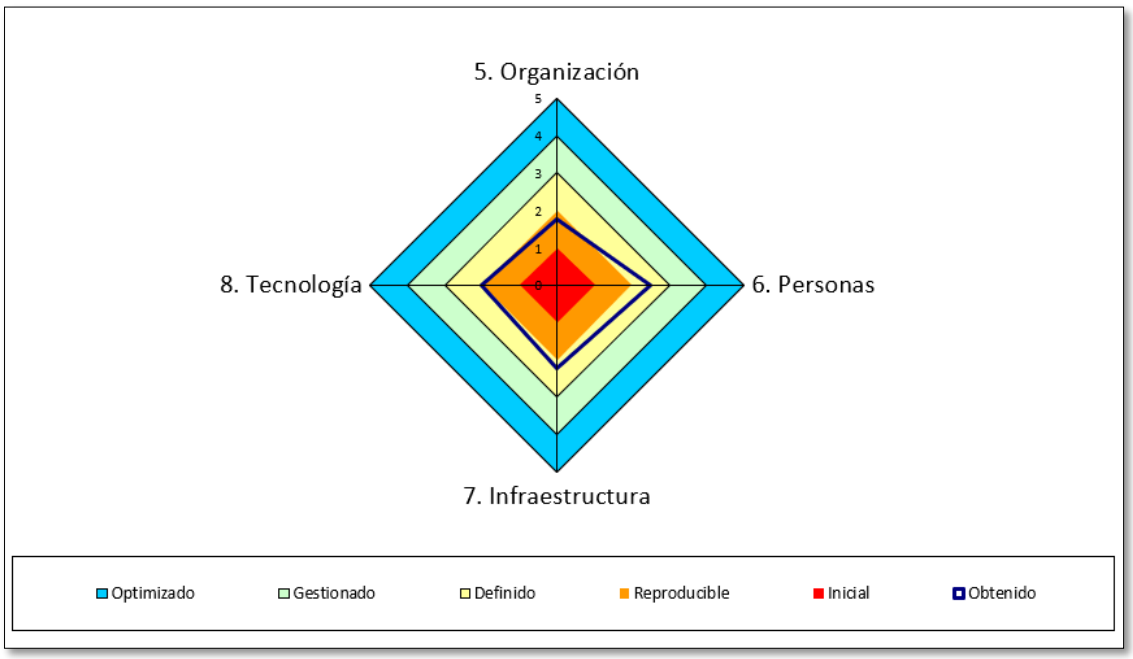


Figura 8. Resultats del anàlisi GAP dels controls

La línia blava es la situació actual i és pot veure com la majoria dels controls estan en un estat reproduïble. L'estat esperat que es busca aconseguir amb el SGSI seria, al menys, el color verd (gestionat). Però sempre s'ha de tenir en compte que l'òptim estaria en el blau cel (optimitzat).

**Secció 5: Organització**

- La cooperativa disposa d'un nivell inicial en la definició de polítiques de seguretat i les responsabilitats de la direcció, però reconeixen un compromís per millorar-ho.
- Es recomana una millora en la clarificació de les responsabilitats i l'establiment de polítiques específiques.
- Les relacions amb autoritats i grups d'informació especials estan en una fase inicial. Per aquesta raó, s'haurien de formalitzar protocols en aquestes àrees per millorar la gestió de la seguretat.
- La cooperativa també reconeix la importància de la segregació de tasques, i es podria millorar per reduir els riscos.

- La gestió d'incidents i la intel·ligència d'amenaces es troben en una fase inicial. Es recomana una millora en la preparació i resposta als incidents de seguretat.

**Secció 6: Persones**

- Malgrat la consciència de la necessitat de formació en seguretat de la informació, es necessita una estructura més clara i una major implementació de processos disciplinaris.
- Les polítiques sobre treball remot són definides, però suggereixen la necessitat de reforçar les pràctiques de seguretat.

**Secció 7: Infraestructura**

- Es disposa d'una infraestructura física definida, però manquen mesures específiques per protegir-se contra amenaces externes i ambientals.
- L'empresa hauria de desenvolupar polítiques més detallades sobre la gestió dels equips i les instal·lacions, així com millorar els controls de seguretat física.

**Secció 8: Tecnologia**

- Cal una millora en la gestió de privilegis d'accés i restriccions d'accés a la informació.
- Es recomana desenvolupar polítiques i controls més definits per a la seguretat dels dispositius i el programari, així com per a la prevenció de fuites de dades i còpies de seguretat de la informació.
- En general, la cooperativa ha identificat àrees clau de millora en la seva implementació de controls de seguretat de la informació. Es recomana desenvolupar i implementar polítiques més detallades, establir processos disciplinaris i reforçar les pràctiques de seguretat física i tecnològica per millorar la seva maduresa en seguretat de la informació i reduir els riscos associats.

El resultat d'aquest anàlisi GAP està adjunt en l'Annex 2 de la memòria.

# 3. Sistema de Gestió Documental

## 3.1 Política de Seguretat

La Política de Seguretat és un document essencial establert per la alta direcció conforme als requisits de la norma ISO 27001:2023. Aquest document és defineix en l'etapa *plan* del PDCA i proporciona un marc de referència per a la protecció de la informació dins de la cooperativa i ha de complir amb els següents criteris:

- Preservar la confidencialitat de la informació sensible, assegurant que només les persones autoritzades tinguin accés a la mateixa.
- Garantir la integritat de les dades, assegurant que la informació no es modifiqui ni es corrompi sense autorització.
- Mantenir la disponibilitat dels sistemes i recursos de la cooperativa, assegurant que estiguin accessibles quan sigui necessari.
- Garantir el procés de millor continua i la revisió periòdica del SGSI.
- Aplicació dels controls adequats per preservar la seguretat de la informació.
- Complir amb les lleis, regulacions i altres requisits aplicables relacionats amb la seguretat de la informació segons el marc normatiu (ISO 27001:2023, LOPDGDD i RGPD).

**Àmbit:**
La política de seguretat s'aplica a tots els sistemes, recursos i dades de la cooperativa, incloent-hi les aplicacions internes, les dades dels clients i els recursos de tecnologia de la informació. Per tant, les mesures seran organitzatives, físiques i lògiques, adaptant-se a tots els recursos i processos.

**Principis:**
La política de seguretat està fonamentada pels principis de transparència a més de garantir la confidencialitat, la integritat i la disponibilitat de la informació basant-se en l'estàndard normatiu de la ISO/IEC 27001/2023.

**Marc legal:**
Es compliran totes les lleis, regulacions i altres requisits aplicables relacionats amb la seguretat de la informació segons els següents marcs normatius:

- Normatives ISO 27001:2023 i ISO/IEC 27002:2023
- Llei Orgànica de Dades Digitals i Garantia de Drets Digitals (LOPDGDD)
- Reglament General de Protecció de Dades (GDPR)

**Responsabilitats del personal:**
Tots els membres del personal, incloent-hi empleats, voluntaris, col·laboradors i personal de tercers, tenen la responsabilitat de complir amb aquesta política i les mesures de seguretat establertes.

El personal ha de seguir els procediments i controls de seguretat establerts per protegir la informació de la cooperativa. Tant els empleats com els proveïdors o tercers que accedeixin interna o externament a qualsevol actiu de la informació és responsable de la seva protecció, i notificarà qualsevol situació que pugui posar en risc a la cooperativa o a les persones.

Aquesta Política de Seguretat de la Informació està disponible per al personal de la cooperativa i s'ha de comunicar de manera efectiva dins de l'organització.
Totes les parts interessades, segons sigui apropiat, tindran accés a aquesta política.

**Ús adequat dels recursos de tecnologia de la informació:**
Els recursos i tecnologies de la informació s'han d'utilitzar de manera eficaç i coherent amb els objectius de la cooperativa.
S'han d'aplicar els controls adequats per preservar la seguretat de la informació, incloent-hi l'ús de contrasenyes segures i l'accés limitat als sistemes.

**Implementació:**
La implementació de la política de seguretat requerirà de la formació del personal per garantir la comprensió i adopció de les polítiques de seguretat, l'avaluació sistemàtica de riscos per identificar possibles vulnerabilitats, la implementació de controls de seguretat adequats per mitigar els riscos identificats i la monitorització constant per assegurar el compliment continu de les polítiques i controls establerts. A més, es fomentarà la participació activa del personal en aquest procés per garantir una implementació efectiva i una cultura de seguretat robusta a la cooperativa.

**Organització del SGSI:**
S'establiran rols i responsabilitats específiques per al personal encarregat de supervisar, implementar i mantenir les mesures de seguretat de la informació dins de la cooperativa. Aquests rols són detallats en l'apartat "3.5 Gestió de Rols i Responsabilitats". A més, es promourà una clara comunicació i coordinació entre els diferents departaments i membres de l'organització per garantir una gestió coherent i efectiva de la seguretat de la informació.

**Escenaris**:
Es realitzarà una identificació de possibles escenaris de riscos i amenaces a la seguretat de la informació, incloent-hi atacs cibernètics, pèrdua de dades,

accés no autoritzat, desastres naturals i altres incidents. Per a cada escenari, s'establiran protocols d'actuació i plans de resposta per minimitzar els impactes i protegir la informació de la cooperativa. Aquesta anàlisi s'utilitzarà per millorar les pràctiques de seguretat i preparar el personal per afrontar situacions d'emergència

**Compromís amb la millora continua:**
La cooperativa es compromet a millorar de manera contínua el seu sistema de gestió de la seguretat de la informació mitjançant l'avaluació regular, la revisió i l'actualització de les mesures de seguretat.

**Compromís de la direcció i accions:**
Per garantir una implementació eficaç de la política de seguretat, l'Alta direcció es compromet a impulsar el desenvolupament i l'aplicació de les mesures de seguretat de la informació. A més, s'encarregarà de garantir els recursos necessaris i promoure una cultura de seguretat dins de l'organització. L'Alta direcció també supervisarà el compliment, la divulgació i la revisió periòdica de la política de seguretat.

**Revisió i actualització:**
En cas de revisions de la política de seguretat, les versions anteriors seran derogades i substituïdes per la versió més recent. Les noves revisions seran comunicades a tot el personal.
Aquesta política serà revisada i actualitzada periòdicament (anualment) per garantir la seva eficàcia i rellevància.
Totes les revisions seran aprovades per la direcció de la cooperativa i es comunicaran a tot el personal.
Alhora, pot requerir una revisió abans del termini previst en certes situacions com la materialització d'una incidència important de seguretat o canvis organitzatius rellevants.

**Sancions:**
Les sancions per incompliment de la política de seguretat de la informació inclouen advertències escrites per infraccions menors, formació addicional per manca de comprensió, restricció d'accés en casos greus, accions disciplinàries com a suspensions o rescissió del contracte, responsabilitat legal en violacions de lleis de protecció de dades, i report a autoritats competents per violacions greus.

### 3.2 Procediment d’auditories internes

Les auditories internes són una part essencial del sistema de gestió de la seguretat de la informació (SGSI) de la cooperativa. Aquest procediment estableix les directrius per a la realització d'auditories internes periòdiques per avaluar l'eficàcia i la conformitat del SGSI amb els requisits establerts, així com per identificar àrees d' millora.

**Responsabilitats:**

- **Auditor en cap:** Encarregat principal de dirigir i supervisar l'auditoria. Ha de tenir un coneixement profund del sistema a auditar i és designat per la direcció de l'organització. És responsable d'establir els objectius, l'abast, els criteris i la durada de l'auditoria, així com de designar l'equip d'auditors i tècnics necessaris per a la seva realització. Vetlla perquè l'auditoria es dugui a terme de manera adequada seguint el pla establert.
- **Auditor:** Persona amb coneixements específics de l'àmbit a auditar i comprensió de la legislació i regulacions aplicables. També ha de ser capaç de comprendre les particularitats de l'organització auditada. Opera sota la supervisió del Responsable d'Auditoria i contribueix activament a l'execució de l'auditoria.
- **Tècnics especialistes:** Encarregats de realitzar tasques tècniques específiques durant l'auditoria, especialment quan l'auditor no té els coneixements o habilitats adequades per a aquestes tasques. Treballen sempre sota la supervisió del Responsable d'Auditoria i compleixen un paper crucial en la recopilació de dades i informació tècnica.

**Planificació d'Auditories:**

S'ha de definir un pla d'auditoria que contempli la freqüència i les dates d'execució, l'abast, la metodologia de la mateixa auditoria i l'assignació d'interlocutors per a la planificació, la realització i la presentació d'informes de resultats. Aquest pla ha de comprendre una descripció de les ubicacions físiques, les unitats organitzatives, les activitats i els processos, així com les dates d'inici i finalització.

És important incidir que les auditories internes han de ser realitzades per personal que no hagi participat en la implantació de l'SGSI, per assegurar l'objectivitat i la imparcialitat de l'auditoria i la independència dels auditors.

Es realitzarà una planificació d'auditories periòdiques seguint un criteri preestablert, en consonància amb el sistema de millora continuada tipus PDCA.

L'abast de l'auditoria comprendrà la revisió del sistema de gestió complet, basat en la norma ISO/IEC 27001, així com la revisió d'una selecció de controls implantats a la cooperativa. Aquesta selecció de controls es farà de comú acord entre l'Auditor Cap i el Responsable de l'SGSI, amb la informació de la Declaració d'Aplicabilitat (SoA). A més, cal assegurar que s'han auditat tots els controls de l'Annex A (objectius de control i controls de referència) de la norma ISO 27001 en un cicle de 3 anys.

La periodicitat de les auditories internes serà anual, realitzant-se durant el primer semestre de l'any. Això permetrà dedicar el segon semestre a la realització de l'auditoria externa i, si és necessari, a la correcció de les no conformitats identificades durant les auditories internes.

El programa d'auditories inclourà:

- Una revisió anual de conformitat del SGSI amb els estàndards internacionals de seguretat de la informació.
- Una revisió anual del pla de continuïtat.
- Una auditoria trimestral dels controls de seguretat informàtica.
- Una auditoria anual dels controls de seguretat física a les instal·lacions.
- Una auditoria biennal de protecció de dades de caràcter personal.

El procediment a seguir es basarà en aquestes fases principals:

**1. Planificació del calendari:** En aquesta fase inicial, es coordinarà amb les diferents àrees de l'organització per establir un calendari d'auditories internes que tingui en compte les seves necessitats i disponibilitat. Aquest calendari s'adaptarà al pla de millora continuada del SGSI, assegurant una cobertura adequada de tots els àmbits rellevants.

**2. Reunions preparatòries**: Es duran a terme sessions de treball amb l'equip d'auditors interns i les àrees afectades per revisar l'abast de l'auditoria, definir els objectius específics i establir els criteris d'avaluació. Aquestes reunions serviran també per comunicar clarament les expectatives i requisits de participació en tots els implicats.

**3. Treball de camp:** Durant aquesta fase, l'equip d'auditors realitzarà les activitats d'auditoria segons el calendari establert. Això inclourà la recopilació d'evidències, entrevistes amb el personal rellevant, revisió de

documents i altres tasques necessàries per avaluar l'eficàcia del SGSI i identificar possibles àrees de millora.

**4. Consolidació de resultats:** Un cop finalitzat el treball de camp, es revisarà i analitzarà tota la informació recopilada per identificar les no conformitats, les observacions positives i les recomanacions de millora. Aquesta fase també inclourà l'elaboració d'un informe executiu que ressalti els punts claus i les accions correctives proposades.

**Execució d'Auditoria interna**

Per garantir una execució precisa de l'auditoria, l'auditor comunicarà anticipadament als responsables de les àrees sotmeses a l'auditoria interna sobre el procés i sol·licitarà la documentació pertinent amb prou antelació per a la seva revisió i posterior desenvolupament durant l'auditoria.

L'Auditoria Interna del SGSI comprendrà dues parts principals:

- **Revisió del sistema de gestió:** aquesta fase implica l'anàlisi de la documentació rellevant, la revisió del marc de gestió del SGSI, incloent-hi el context, l'abast, l'anàlisi i la gestió del risc, la declaració d'aplicabilitat (SoA), la política de seguretat, els rols de seguretat, la gestió de no conformitats, el quadre de comandament, entre altres aspectes.

- **Proves de compliment:** en aquesta etapa, es verifica el grau d'implementació i eficàcia dels controls de seguretat a través de diverses activitats com entrevistes amb els propietaris d'actius, els responsables de processos de negoci, els usuaris directes o indirectes del SGSI, així com la revisió de les àrees de risc, la comprovació del compliment dels objectius i metes establerts, i la revisió de la documentació in situ del sistema, entre altres aspectes.

**Informe dels resultats**

Un cop recollides les evidències necessàries per comprovar el compliment dels diferents apartats i controls de la norma, es genera l'informe d'auditoria interna els resultats del qual han de ser posats en coneixement de la Direcció General, les àrees auditades i del Comitè de Seguretat per a avaluació i tractament a nivell corporatiu.

El responsable de l'SGSI serà l'encarregat d'informar dels resultats obtinguts i del manteniment dels registres derivats de la realització d'auditories internes.

L'informe d'auditoria haurà d'incloure com a mínim els següents elements:

- Data de l'auditoria.
- Nom dels auditors.
- Abast de l'auditoria.
- Controls auditats.
- Conformitat de l'SGSI amb els estàndards internacionals de seguretat de la informació o grau d'adequació.
- No-conformitats detectades.
- Recomanacions de millora.

**Resultats**

Un cop finalitzat l'informe d'auditoria interna, el responsable de l'SGSI haurà d'establir les accions de seguiment per comprovar l'eficàcia de les accions correctives derivades de l'auditoria interna. Aquests plans d'acció han de ser aprovats al màxim nivell possible a l'organització, de manera que es garanteixi la correcció d'aquelles qüestions o processos amb què no s'estigui complint totalment.

La contractació d'un servei d'auditoria externa amb coneixements específics en la matèria que cal auditar és clau perquè la cooperativa d'un informe d'auditoria objectiu, per aquesta raó, es de caràcter obligatori.

### 3.3 Gestió d'indicadors

Per tal de mantenir el SGSI actualitzat i eficaç, s'ha d'establir i avaluar indicadors que permetin controlar el funcionament de les mesures de seguretat implementades. Aquests indicadors no només ens ajuden a mesurar l'eficàcia i eficiència del sistema, sinó també a avaluar la efectivitat dels controls implantats.

Cada indicador consta de diversos components essencials que ens ajuden a definir-lo i gestionar-lo adequadament:

- Nom de l'indicador: Aquest ha de ser significatiu i breu, reflectint clarament el mesurament que es realitza.
- Descripció de l'indicador: S'explica l'objectiu i la finalitat de la mesura.

- Control de seguretat a què dona suport: Especificació dels controls que aquest indicador cobreix.
- Fórmula de mesurament: Es descriu la fórmula utilitzada per calcular la mesura, assegurant que els paràmetres siguin clars i concrets.
- Unitats de mesura: Les unitats de mesura s'especifiquen clarament per a una comprensió precisa dels resultats.
- Freqüència de mesura: Es determina amb quina freqüència es recolliran les dades, tenint en compte la variabilitat temporal.
- Valors objectiu i llindar: Es defineixen els valors esperats i els llindars que activen alarmes en cas de desviacions.
- Responsable de la mesura: S'identifica la persona o el càrrec responsable de proporcionar els resultats de la mesura.

Els indicadors es presenten regularment al Comitè de Seguretat de la Informació (departament que es forma durant la realització del SGSI i ve especificat en el punt 3.5) i a la direcció general de la cooperativa en informes periòdics. Aquests informes inclouen una anàlisi dels indicadors rellevants, destaquen les tendències, les desviacions significatives respecte als objectius establerts i presenten les accions correctives i de millora proposades.

Per tant, els indicadors es controlen i es revisen periòdicament per assegurar la seva exactitud i fiabilitat. Es manté un registre detallat de les dades recollides, els càlculs realitzats i els resultats obtinguts. En cas de detectar alguna anomalia o desviació respecte als llindars establerts, s'actua ràpidament per identificar les causes subjacents i es prenen les accions correctives adequades per corregir-les.

| **Nom - ID** | | **Rols i Responsabilitats – ID001** | |
|---|---|---|---|
| Descripció | | Aquest indicador mesura el grau de definició i assignació de rols i responsabilitats relacionades amb la gestió de la seguretat de la informació a l'organització. | |
| Controls relacionats | | 7.1.1 Responsabilitats en matèria de seguretat de la informació<br>7.2.1 Funciones i obligacions<br>7.2.2 Segregació de funcions | |
| Fórmula de mesurament | | Nº rols i responsabilitats definits i assignats / Total de rols i responsabilitats previstos | |
| Unitats de mesura | | Percentatge (%) | |
| Freqüència de mesura | | Trimestral | |
| V. Objectiu | Llindar | 90% | < 80% |
| Responsable | | Responsable de seguretat de la informació | |

Taula 4. Indicador ID001

| Nom - ID | | Control i gestió dels actius – ID002 | |
|---|---|---|---|
| Descripció | | Mesura l'eficàcia del control i gestió dels actius de la cooperativa | |
| Controls relacionats | | 5.9 Inventari d'informació i altres actius associats<br>5.10 Ús acceptable de la informació i actius associats<br>5.11 Devolució d'actius<br>5.12 Classificació de la informació.<br>8.1 Dispositius finals de l'usuari<br>8.6 Gestió de capacitats<br>8.9 Gestió de configuració<br>9.1 Gestió de l'ús | |
| Fórmula de mesurament | | Nº d'actius registrats i classificats correctament / Nº total | |
| Unitats de mesura | | Percentatge (%) | |
| Freqüència de mesura | | Mensual | |
| V. Objectiu | V. Objectiu | 100% | < 95% |
| Responsable | | Responsable de seguretat de la informació | |

Taula 5. Indicador ID002

| Nom - ID | | Revisió d'accés a les xarxes i sistemes – ID003 | |
|---|---|---|---|
| Descripció | | Mesura l'eficàcia dels controls d'accés implementats per garantir que només els usuaris autoritzats poden accedir a les xarxes, serveis i aplicacions de l'empresa, reduint així el risc de violacions de seguretat i la pèrdua de dades sensibles. | |
| Controls relacionats | | 8.2 Gestió de privilegis d'accés<br>8.3 Restricció del accés a la informació<br>8.5 Autenticació segura<br>8.15 Registres d'esdeveniments | |
| Fórmula de càlcul | | Percentatge d'accés autoritzat vs. total d'intents d'accés | |
| Unitats de càlcul | | Percentatge (%) | |
| Freqüència de mesura | | Mensual | |
| V. Objectiu | Llindar | 100% | < 90% |
| Responsable | | Responsable de seguretat de la informació | |

Taula 6. Indicador ID003

| Nom - ID | | Seguretat en el Teletreball – ID004 | |
|---|---|---|---|
| Descripció | | Mesura el nivell de seguretat implementat durant el teletreball per garantir la protecció de la informació de l'empresa fora de les instal·lacions físiques | |
| Controls relacionats | | 6.7 Teletreball<br>7.9 Seguridad dels equips fora les instal·lacions | |
| Fórmula de càlcul | | Puntuació del 0 al 10 | |
| Unitats de càlcul | | Numèrica | |
| Freqüència de mesura | | Mensual | |
| V. Objectiu | Llindar | 10 | 10 |
| Responsable | | Responsable de seguretat de la informació | |

Taula 7. Indicador ID004

| Nom - ID | | Revisió de Polítiques de Seguretat – ID005 | |
|---|---|---|---|
| Descripció | | Aquest indicador mesura l'eficàcia de la revisió i mesura de les polítiques de seguretat de la informació a l'organització. | |
| Controls relacionats | | 5.1 Polítiques per a la seguretat de la informació<br>5.4 Responsabilitats de la direcció<br>5.31 Identificació de requisits legals, reglamentaris i contractuals<br>6.5 Responsabilitat davant la finalització o canvi<br>5.35 Revisió independent de la seguretat de la informació | |
| Fórmula de càlcul | | Nombre de polítiques de seguretat revisades i mesurades / Nombre total de polítiques de seguretat de la informació | |
| Unitats de càlcul | | Percentatge (%) | |
| Freqüència de mesura | | Trimestral | |
| V. Objectiu | Llindar | 100% | 100% |
| Responsable | | Responsable de seguretat de la informació i la direcció | |

Taula 8. Indicador ID005

| Nom - ID | | Accessos als sistemes no autoritzats – ID006 | |
|---|---|---|---|
| Descripció | | Aquest indicador mesura la freqüència d'intents d'accés no autoritzats als sistemes i a la informació sensible de l'empresa. Aquests intents poden indicar possibles vulnerabilitats en els controls d'accés i amenaçar la confidencialitat i la integritat de la informació. | |
| Controls relacionats | | 8.3 Restricció del accés a la informació<br>8.5 Autenticació segura<br>8.15 Registres d'esdeveniments | |
| Fórmula de càlcul | | Nombre d'intents d'accés no autoritzats | |
| Unitats de càlcul | | Nombre d'intents | |
| Freqüència de mesura | | Setmanal | |
| V. Objectiu | Llindar | 0 | 0 |
| Responsable | | Responsable de seguretat de la informació | |

Taula 9. Indicador ID006

| Nom - ID | | Classificació de la informació – ID007 | |
|---|---|---|---|
| Descripció | | Mesura l'eficàcia del sistema de classificació de la informació de l'empresa per garantir que s'apliquen les mesures de seguretat adequades segons la seva importància i sensibilitat. | |
| Controls relacionats | | 5.12 Classificació de la informació<br>5.13 Etiquetatge de la informació<br>5.33 Protecció dels registres | |
| Fórmula de càlcul | | Percentatge d'informació classificada correctament | |
| Unitats de càlcul | | Percentatge (%) | |
| Freqüència de mesura | | Mensual | |
| V. Objectiu | Llindar | 100% | < 95% |
| Responsable | | Responsable de seguretat de la informació | |

Taula 10. Indicador ID007

| Nom - ID | | Seguretat física de les instal·lacions – ID008 | |
|---|---|---|---|
| Descripció | | Mesura el nivell de seguretat física de les instal·lacions de l'empresa per protegir els actius, la informació i el personal contra accés no autoritzat, robatoris o danys. | |
| Controls relacionats | | 7.1 Perímetre de seguretat física<br>7.2 Controls físics d'entrada<br>7.3 Seguretat d'oficines, despatxos i recursos<br>7.4 Monitorització de la seguretat física<br>7.5 Protecció contra les amenaces físiques i ambientals | |
| Fórmula de càlcul | | Percentatge de conformitat amb els controls de seguretat | |
| Unitats de càlcul | | Percentatge (%) | |
| Freqüència de mesura | | Mensual | |
| V. Objectiu | Llindar | 100% | 100% |
| Responsable | | Empresa subcontractada de seguretat física | |

Taula 11. Indicador ID008

| Nom - ID | | Temps mitjà de detecció i resposta incidents – ID009 | |
|---|---|---|---|
| Descripció | | Aquest indicador mesura el temps mitjà que triga l'organització a detectar i respondre a incidents de seguretat de la informació des que es produeixen. | |
| Controls relacionats | | 5.24 Planificació i preparació de la gestió d'incidents de seguretat de la informació<br>5.25 Avaluació i decisió sobre els esdeveniments de seguretat de la informació<br>5.26 Resposta a incidents de seguretat de la informació<br>5.27 Aprenentatge dels incidents de seguretat de la informació | |
| Fórmula de càlcul | | Temps mitjà (en hores o dies) | |
| Unitats de càlcul | | Hores o dies | |
| Freqüència de mesura | | Mensual | |
| V. Objectiu | Llindar | < 12h | < 24h |
| Responsable | | Equip de resposta a incidents de seguretat de la info. | |

Taula 12. Indicador ID009

| Nom - ID | | Manteniment dels equips – ID010 | |
|---|---|---|---|
| Descripció | | Mesura l'eficàcia del manteniment dels equips informàtics i altres actius relacionats amb la tecnologia de la informació. | |
| Controls relacionats | | 7.13 Manteniment dels equips<br>8.10 Eliminació de la informació<br>8.13 Còpies de seguretat de la informació | |
| Fórmula de càlcul | | Índex de Manteniment = (Nombre d'equips sotmesos a manteniment correctiu i preventiu en temps i forma / Nombre total d'equips) x 100 | |
| Unitats de càlcul | | Percentatge (%) | |
| Freqüència de mesura | | Mensual | |
| V. Objectiu | Llindar | 100% | < 95% |
| Responsable | | Responsable del manteniment | |

Taula 13. Indicador ID010

| Nom - ID | | Compliment d'auditories – ID011 | |
|---|---|---|---|
| Descripció | | Mesura el grau de conformitat de l'empresa amb les recomanacions o les troballes identificades en les auditories internes o externes | |
| Controls relacionats | | 5.35 Revisió independent de la seguretat de la informació<br>6.4 Procés disciplinari<br>6.5 Responsabilitat davant la finalització o el canvi | |
| Fórmula de càlcul | | Índex de Compliment = (Nombre de recomanacions o troballes implementades / Nombre total de recomanacions o troballes) * 100 | |
| Unitats de càlcul | | Percentatge (%) | |
| Freqüència de mesura | | Trimestral | |
| V. Objectiu | Llindar | 95% | < 90% |
| Responsable | | Responsable del departament d'auditoria | |

Taula 14. Indicador ID011

### 3.4 Procediment de revisió per direcció

En aquest apartat, es descriurà el procediment de revisió per direcció implementat a l'organització per avaluar la eficàcia i adequació del SGSI segons els requisits del punt 9.3 de la normativa ISO 27001:2023.

El procediment de revisió per direcció té com a objectiu avaluar periòdicament la eficàcia i adequació del SGSI de la cooperativa, garantint la seva idoneïtat per protegir la informació sensible i assegurar el compliment dels requisits de seguretat. Aquesta revisió, ha d'incloure les consideracions següents:

- L'estat de les accions estimades sorgides de les revisions prèvies fetes per part de la direcció.
- Els canvis tant en les qüestions internes i externes que siguin pertinents als sistemes de gestió de la seguretat de la informació des de la última revisió.
- La informació sobre el comportament de la seguretat de la informació, incloent:
    - No conformitats i accions correctives.
    - Seguiment i resultat de les mesures.
    - Resultats de les auditories.
    - El compliment dels objectius de seguretat de la informació.
- Els comentaris provinents de les parts interessades.
- Els resultats de les apreciacions dels riscos i l'estat del pla de tractament de riscos.

- Les oportunitats de millora continua.

**Responsables:** Els responsables d'executar aquest procediment són la direcció de l'organització, el Cap d'Informàtica (CIO) del departament I.T i el Cap de Seguretat de la Informació (CISO) creat per al SGSI, ja que tenen la responsabilitat de supervisar i garantir la seguretat de la informació a tots els nivells de l'organització.

L'informe resultant de la revisió ha de contenir les resolucions pertinents respecte a les oportunitats de millora i qualsevol necessitat de modificació en el SGSI. És imprescindible conservar la documentació com a prova de les revisions realitzades per la direcció.
Aquestes revisions han de dur-se a terme de manera regular, sense superar mai un any entre elles. En cas que es produeixi un canvi substancial en els requisits que afectin el SGSI, serà necessària una nova revisió.
En cas que hi hagi un procediment de revisió anterior, aquest serà derogat i substituït pel present procediment. Tot i això, si és la primera vegada que s'implementa un procediment de revisió per direcció, no serà necessari abordar aquest punt.

L'efectivitat del procediment de revisió per direcció es mesura mitjançant la revisió regular de la conformitat amb els objectius de seguretat de la informació i l'avaluació de les oportunitats de millora identificades. Això es realitza amb l'ús d'indicadors clau de rendiment (el punt 3.3 anterior), com ara la reducció de no conformitats, l'augment del compliment dels objectius de seguretat i l'eficàcia de les accions correctives implementades.

### 3.5 Gestió de rols i responsabilitats

El SGSI requereix la creació i manteniment d'un equip dedicat a supervisar i millorar la seguretat de la informació a l'organització. Aquest equip, conegut com a Comitè de Seguretat, s'ubicarà en el departament de Gestió i Administració de l'organigrama de la cooperativa i estarà compost per membres actuals de l'organització del departament T.I que rebran la formació pertinent així com la contractació de personal nou addicional que ocupi el rol en cas necessari. Aquesta inclusió garanteix que les decisions preses per l'equip estiguin alineades amb els objectius i les polítiques de l'alta direcció, i que puguin ser aprovades prèviament per un membre de la direcció.

**Comitè de Seguretat**

Departament responsable de supervisar totes les activitats relacionades amb la seguretat de la informació, des de l'establiment de polítiques fins a la implementació de controls i la resposta a incidents. Està format per:

- **Director General (CEO - *Chief Executive Officer*):** Membre de la actual direcció general i responsable últim de vetllar pel compliment dels objectius de seguretat de la informació i de garantir que aquesta àrea estigui alineada amb la visió i els objectius globals de l'empresa. A més, tindria autoritat per aprovar decisions importants i per assignar recursos necessaris per implementar mesures de protecció adequades.
- **El director de seguretat de la informació (CISO - *Chief Information Security Officer*):** Professional contractat per actuar com a líder del Comitè de Seguretat i té la responsabilitat general de supervisar totes les iniciatives i els programes relacionats amb la seguretat de la informació de la cooperativa. Ha d'establir la visió i l'estratègia de seguretat, la gestió dels riscos de seguretat, la supervisió de la implementació de controls de seguretat i la coordinació de la resposta a incidents.
- **El director de sistemes de informació (CIO - *Chief Information Officer):***Cap de l'àrea T.I, el CIO és responsable de dirigir les estratègies tecnològiques de l'empresa cooperativa. Col·labora amb el CISO i altres membres del Comitè per assegurar que les iniciatives s'alineïn amb els objectius de la organització
- **Responsable T.I (CTO - *Chief Technology Officer*):** Membre format de l'àrea T.I que porta la seva experiència tècnica per assegurar la implementació adequada de les mesures de seguretat de la informació als sistemes i les infraestructures tecnològiques de l'empresa. Col·labora amb el CISO per garantir que els sistemes informàtics i les xarxes estiguin protegits adequadament.
- **Delegat de privadesa (DPD - *Data Protection Officer*):** És responsable de garantir el compliment de les normatives de protecció de dades dins de l'organització, assegurant-se que les polítiques i pràctiques de privacitat siguin adequadament implementades i seguides.
- **Auditor intern de seguretat:** Professional contractat per a ser el responsable de supervisar i millorar la seguretat de la informació, identificant àrees d'optimització i avaluar l'eficàcia dels controls de seguretat. Assegura el compliment dels estàndards de seguretat i ofereix una avaluació imparcial del programa de seguretat per mantenir la conformitat amb les normatives i protegir actius.

- **Empresa subcontractada de seguretat física**: Es considerada com a part integral del Comitè de Seguretat, ja que contribueix en gran mesura a la protecció dels actius físics de l'organització. Els representants d'aquesta empresa participen en les reunions per assegurar una coordinació adequada entre les iniciatives de seguretat física i de seguretat de la informació.
- **Responsable de Recursos Humans:** Membre de l'àrea de RRHH. És responsable de vetllar per la seguretat de la informació en el procés de contractació, formació i gestió del personal. Assegura que els empleats estiguin ben informats sobre les polítiques de seguretat de la informació i compleixin amb els requisits de seguretat establerts per l'empresa.
- **Representant dels empleats**: Aquest membre aportaria una perspectiva important sobre les necessitats i preocupacions del personal de la cooperativa, especialment en relació amb l'ús diari de sistemes i aplicacions informàtiques.

Per garantir una supervisió efectiva de les qüestions de seguretat, el Comitè de Seguretat mantindrà reunions trimestrals programades, però es podran convocar reunions addicionals segons sigui necessari per abordar qüestions urgents o importants. També s'han de documentar els temes tractats, les decisions preses i qualsevol acció acordada. Aquesta documentació servirà com a registre històric de les activitats del comitè i facilitarà la revisió i el seguiment del progrés en matèria de seguretat de la informació."

### 3.6 Metodologia d'anàlisi de riscos

És imprescindible reconèixer els actius d'informació i avaluar els riscos associats a ells, considerant l'impacte potencial per a l'organització si es compromet la confidencialitat, la privadesa, la integritat o la disponibilitat d'aquests actius. Aquesta anàlisi de riscos permet a la direcció prendre decisions informades sobre el nivell de risc que l'organització està disposada a assumir, i prioritzar les accions en seguretat de la informació, garantint sempre l'adopció de mesures proporcionades.

Segons el PDF "Implantació d'un SGSI" esmentat en la bibliografia, les pautes d'implantació són:

- L'anàlisi de riscos ha de ser formal i estar documentada.
- La complexitat de l'anàlisi de riscos depèn de la criticitat dels actius que cal protegir.

- La metodologia utilitzada ha de ser coherent amb la complexitat i els nivells de protecció requerits.
- El grau de profunditat amb què s'ha de dur a terme l'anàlisi de riscos varia segons la maduresa de l'organització. Per a fer els primers passos es recomana fer una anàlisi d'alt nivell dels processos inclosos en l'abast, amb l'objectiu de detectar els punts de màxim risc. Més endavant, si escau, es pot fer una anàlisi més profunda dels processos inclosos en l'abast que es considerin més crítics.
- Ha de cobrir tot l'abast de l'SGSI.
- Els riscos canvien constantment, de manera que hi ha d'haver una metodologia i un procediment per a revisar-los i fer-ne el manteniment.
- La direcció ha d'aprovar formalment el risc residual, cosa que ha de quedar recollida en un document, que constitueix un "registre" de l'SGSI.

Per avaluar els riscos de la cooperativa durant el SGSI, s'ha escollit la metodologia **MAGERIT**, que va ser elaborada pel Ministeri d'Administracions Públiques (MAP) amb la finalitat d'ajudar a totes les administracions públiques de l'Estat espanyol. Això no obstant, aquesta metodologia es pot aplicar a qualsevol organització, independentment que sigui a l'Estat espanyol o en un altre país, i ofereix una base sòlida i reconeguda per a la gestió de riscos. A més, la classificació d'amenaces ofereix totes les possibilitats necessàries per a la cooperativa, cobrint de manera satisfactòria l'anàlisi.

L'anàlisi de riscos MAGERIT és una aproximació metòdica per determinar el risc seguint aquesta sèrie de passos pautats: Pas 1. Actius / Pas 2. Amenaces / Pas 3. Salvaguardes / Pas 4. Impacte Residual / Pas 5. Risc Residual
Per a aquest cas, utilitzarem les següents fases necessàries en el nostre SGSI de la cooperativa, que es defineixen d'aquesta manera:

**Fase 1. Identificació dels Actius**

Determinar els actius rellevants per a la cooperativa, la seva interrelació i el seu valor, en el sentit de quin perjudici (cost) en suposaria la degradació.
MAGERIT classifica els actius segons si son:

- Dades (D).
- Claus Criptogràfiques (KY).
- Serveis (S).
- Aplicacions informàtiques (SW).
- Equips informàtics (HW).
- Suports de informació (MED).

- Equipament auxiliar (AUX).
- Xarxes de comunicació (COM).
- Instal·lacions (L).
- Persones (P).

Les dependències entre els actius són necessàries per entendre la seva interrelació i la seva importància per a la seguretat. Els actius essencials com la informació i els serveis depenen d'altres actius com els equips, les comunicacions i el personal. Aquests actius formen una estructura jeràrquica on la seguretat dels actius superiors depèn dels actius inferiors. Això significa que els actius inferiors són fonamentals per sustentar la seguretat dels superiors.

| GRAUS DE DEPENDÈNCIA | | |
|---|---|---|
| 100% | Molt Alta (MA) | Seria impossible treballar en l'actiu dependent |
| 75% | Alta (A) | Seria molt difícil treballar en l'actiu dependent |
| 50% | Mitjana (M) | Se podria treballar en l'actiu dependent però amb moltes dificultats |
| 25% | Baix (B) | Se podria treballar en l'actiu però no seria òptim |
| 0% | Molt baix (MB) | No afecta de cap manera |

Taula 15. Taula graus de dependència

D'un actiu pot interessar calibrar diferents **dimensions**:

- Confidencialitat: Quin dany causaria si ho conegués algú que no hauria de tenir accés? Aquesta valoració és típica en dades.

- Integritat: Quin perjudici causaria si estigués danyat o corromput? Aquesta valoració és típica de les dades, que poden estar manipulades, ser total o parcialment falses o, fins i tot, faltar dades.
- Disponibilitat: Quin perjudici causaria no tenir-lo o no poder utilitzar-lo? Aquesta valoració és típica dels serveis.

- Autenticitat: Quin perjudici causaria no saber exactament qui fa o ha fet cada cosa? Aquesta valoració és típica dels serveis (autenticitat de l'usuari) i de les dades (autenticitat de qui accedeix a les dades per escriure o, simplement, consultar).

- Traçabilitat de l'ús del servei: Quin dany causaria no saber a qui se li presta tal servei? O sigui, qui fa què i quan?
  Traçabilitat de l'accés a les dades: Quin dany causaria no saber qui accedeix a quines dades i què fa amb elles?

Pel que fa a la **valoració**, MAGERIT estableix que:

- Valoració d'actius: Teòricament val qualsevol escala de valors, sempre que sigui comú en totes les dimensions, sigui logarítmica i homogènia. P.E: 0 / 1-2 / 3-5 / 6-8 / 9 / 10 si es quantitativa, i si es qualitativa: menyspreable, baix, mitjà, alt, molt alt, extrem.

- Valoració és econòmica: Es parla de diners. Però sovint la valoració és qualitativa, i queda a discreció de l'usuari; és a dir, responent a criteris subjectius.

- Valoració d'amenaces: La degradació pot valorar-se de forma qualitativa segons: molt baixa, baixa, mitjana, alta i molt alta. La probabilitat segons: molt poc freqüent, poc freqüent, normal, freqüent i molt freqüent

| ESCALA DE VALORS PER A CADA 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 |

Taula 16. Escala de valors per a cada dimensió

### Fase 2. Anàlisi d'amenaces

Les amenaces son "coses que ocorren", i de tot el que pot ocórrer, el que ens interessa ser es allò que li pot causar danys i acabar afectant negativament. Aquestes, s'agrupen segons si són:

- D'origen natural.
- Del entorn (origen industrial).
- Defectes de les aplicacions.
- Causades per persones de forma accidental.
- Causades per persones de forma deliberada.

Un cop s'identifiqui una amenaça que pugui afectar un actiu, és important avaluar la seva influència en el valor d'aquest actiu des de dues perspectives:

- Degradació: aquest aspecte considera com afectaria la pèrdua de valor de l'actiu en cas de ser perjudicat per la amenaça.

| TAULA DE DEGRADACIÓ | | |
|---|---|---|
| 100% | Molt Alta (MA) | L'actiu queda totalment inservible |
| 75% | Alta (A) | L'actiu està pràcticament inservible |
| 50% | Mitjana (M) | Funcionalment degradat amb un rendiment baix |
| 25% | Baixa (B) | Lleugera degradació que no impedeix el funcionament |
| 0% | Molt baixa (MB) | Actiu en perfecte estat |

Taula 17. Taula de degradació

- Probabilitat: aquí s'avalua quan probable o improbable és que la amenaça es materialitzi.

| TAULA DE PROBABILITAT | | | |
|---|---|---|---|
| 100% | 10 | Molt Alta (MA) | Molt freqüent (a diari) |
| 75% | 7,5 | Alta (A) | Freqüent (mensualment) |
| 50% | 5 | Mitjana (M) | Normal (un cop a l'any) |
| 25% | 2,5 | Baixa (B) | Poc freqüent (cada diversos anys) |
| 0,1% | 0,1 | Molt baixa (MB) | Molt poc freqüent (segles) |

Taula 18. Taula de probabilitat

### Fase 3. Estimació de l'impacte

S'anomena impacte a la mida del dany sobre l'actiu derivat de la materialització d'una amenaça. Coneixent el valor dels actius (en diverses dimensions) i la degradació que causen les amenaces, és directe derivar l'impacte que tindrien sobre el sistema.

Impacte = Valor x Degradació

| TAULA D'IMPACTE | | |
|---|---|---|
| 10 | Molt Alt (MA) | Un impacte crític |
| 7,5 | Alt (A) | Un impacte molt important |
| 5 | Mitjà (M) | Un impacte considerable |
| 2,5 | Baix (B) | Un impacte lleu |
| 0,25 | Molt baix (MB) | Gairebé inexistent |

Taula 19. Taula d'impacte

**Pas 4. Estimació del risc**

El risc és la mida del dany probable sobre un sistema. Coneixent l'impacte de les amenaces sobre els actius, és deriva directament el risc només tenint en compte la probabilitat d'ocurrència.
El risc creix amb l'impacte i amb la probabilitat, i es pot distingir una sèrie de zones que cal tenir en compte en el tractament del risc.
A continuació, hi ha una taula extreta de Magerit que ens permet calcular el risc mitjançant la combinació de la probabilitat i l'impacte. D'aquesta manera, es pot comprar posteriorment quin és el risc inicial a través d'aquesta comparativa directa.

| **RISC** Prob x Impacte | | **PROBABILITAT** | | | | |
|---|---|---|---|---|---|---|
| | | Molt baixa | Baixa | Mitjana | Alta | Molt Alta |
| **IMPACTE** | Molt Alt | 5 | 6,25 | 7,5 | 8,75 | 10 |
| | Alt | 3,75 | 5 | 6,25 | 7,5 | 8,75 |
| | Mitjà | 2,5 | 3,75 | 5 | 6,25 | 7,5 |
| | Baix | 1,25 | 2,5 | 3,75 | 5 | 6,25 |
| | Molt baix | 0 | 1,25 | 2,5 | 3,75 | 5 |

Taula 19. Càlcul del risc

**Risc inicial:** És el risc en el que està exposada la cooperativa tenint en compte les mesures de seguretat del moment

**Nivell de risc acceptable**: La cooperativa té com ombrall de risc acceptable el valor de 15. Això significa que si es igual o menor a aquest valor, s'assumirà el risc. Però si es més gran s'haurà de mitigar, reduir o eliminar.

**Risc residual:** És el risc resultant després d'aplicar els plans de tractament i mitigar els riscos que no són acceptables.

### 3.7 Declaració d'aplicabilitat

La Declaració d'Aplicabilitat, o també anomenada SoA (*Statement of Applicability*), és un document fonamental en el marc de la norma ISO 27001:2023, ja que proporciona una descripció detallada dels controls de seguretat de la informació necessaris per gestionar els riscos de manera efectiva. Aquesta declaració inclou els controls seleccionats i específica per a cadascun d'ells si és d'aplicació o no a la cooperativa, amb una justificació, i també esmenta aquells controls que ja estan implementant actualment.

A la normativa ISO/IEC 27001 ve definit que les organitzacions han de determinar quins són els controls necessaris dins de l'abast del SGSI, per tant, serveix com una guia clau per a la implementació efectiva de mesures de seguretat de la informació dins de l'organització, garantint la protecció dels seus actius i la gestió eficaç dels seus riscos de seguretat.

El camps que conté són "Secció | Control | Aplicabilitat | Estat actual | Nivell de compliment | Comentaris". I per a un major enteniment, s'explicaran aquests dos que poden portar certa subjectivitat:

**Estat actual:**

- Implementat: Indica que el control o mesura ja s'ha posat en pràctica i està plenament actiu dins de l'organització.
- En implementació: S'utilitza quan el control o mesura està en procés d'implementació, però encara no està completament actiu o no s'ha desplegat del tot.

**Nivell de compliment:**

- Alt: Indica un compliment complet del control o mesura, sense cap àrea d'insatisfacció o falta.
- Mitjà: S'utilitza quan hi ha un compliment parcial del control o mesura, indicant que s'han assolit alguns dels objectius, però encara hi ha àrees que necessiten millora.
- Baix: Es refereix a un estat en el qual el compliment o la implementació del control està en curs. Pot indicar que s'estan realitzant esforços per millorar el compliment o implementació, però encara no s'ha arribat a un nivell satisfactori.

La declaració d'aplicabilitat està a l'Annex 3.

# 4. Anàlisis de Riscos

## 4.1 Anàlisi i valoració de l'inventari d'actius

L'inventari d'actius de la cooperativa també ve explicat en el punt 2.1, ja que forma part de la descripció detallada de l'organització en ser l'element principal a protegir durant el SGSI. Aquests actius venen agrupats en la següent taula segons la metodologia MAGERIT.

Per iniciar amb l'anàlisi de riscos, revisarem els processos associats i quins graus de dependència tenen els actius. Aquesta valoració es farà a través dels rangs de valors de la "Taula 15 Graus de dependència" del punt 3.6 Metodologia d'anàlisi de riscos.

La dependència es realitzarà mitjançant la relació entre els actius i els processos associats del sistema d'informació de la cooperativa. Aquesta relació reflecteix la importància de l'actiu en el suport i el funcionament dels processos clau de l'organització. Les dependències s'estableixen en funció de com cada actiu contribueix a la realització dels processos, quins processos depenen directament o indirectament de l'actiu per al seu funcionament, i la relació general entre l'actiu i els processos de la organització.

| DEPENDÈNCIES ENTRE ELS ACTIUS | | | | |
|---|---|---|---|---|
| **Tipus** | **Actiu** | **Processos associats** | **Dependència** | **Justificació** |
| **Dades (D)** | Informació dels membres | Dades dels membres, Treballadors, Clients | Molt Alta (MA) | Aquesta informació és crítica per a la cooperativa, ja que inclou dades personals dels membres, treballadors i clients. |
| **Dades (D)** | Dades dels clients | Dades dels clients, Clients | Molt Alta (MA) | La informació dels clients és essencial per al funcionament de la cooperativa, ja que conté detalls sobre els seus clients. |
| **Dades (D)** | Informació financera | Dades financeres | Molt Alta (MA) | Les dades financeres són crucials per a la gestió financera de la cooperativa i han de protegir-se amb el màxim nivell de seguretat. |
| **Dades (D)** | Registres nòmines | Dades dels treballadors, Treballadors | Mitjana (M) | Encara que és important, la seva pèrdua no tindria un impacte tan gran com |

| | | | | |
|---|---|---|---|---|
| | | | | la informació dels membres o dels clients. |
| **Dades (D)** | Còpies de seguretat | Gestió de còpies de seguretat | Mitjana (M) | Les còpies de seguretat són importants però el seu impacte en la continuïtat del negoci és menor que altres actius. |
| **Claus criptogràfiques (KY)** | Claus d'encriptació portàtils | Seguretat de les claus criptogràfiques | Baix (B) | Les claus d'encriptació portàtils tenen un impacte baix ja que la seva pèrdua no compromet directament la confidencialitat dels actius. |
| **Serveis (S)** | VPN | Accés remot, Seguretat de la xarxa | Alta (A) | El VPN és crucial per garantir la seguretat de les connexions remotes i protegir la xarxa de la cooperativa. |
| **Serveis (S)** | Directori Actiu | Gestió d'usuaris, Control d'accés, Autenticació | Molt Alta (MA) | El Directori Actiu és fonamental per gestionar els usuaris i controlar l'accés als recursos, és per això que la seva dependència és molt alta. |
| **Serveis (S)** | Web | Gestió del lloc web, Comunicació amb clients | Alta (A) | El lloc web és un canal important per a la comunicació amb els clients i la seva disponibilitat és crucial per al negoci. |
| **Serveis (S)** | Correu O365 | Comunicació interna, Gestió de correu electrònic | Alta (A) | El correu electrònic és un dels mitjans principals de comunicació interna i externa de la cooperativa, i la seva disponibilitat és crítica. |
| **Hardware (HW)** | Servidors | Gestió dels servidors, Emmagatzematge de dades | Molt Alta (MA) | Els servidors són la infraestructura clau per a l'emmagatzematge i la gestió de les dades de la cooperativa, i la seva indisponiblitat afectaria greument les operacions. |
| **Hardware (HW)** | Portàtils | Gestió d'equips informàtics, Mobilitat dels treballadors | Alta (A) | Els portàtils són importants per a la mobilitat dels treballadors i la seva disponibilitat és crucial per al seu bon funcionament. |

| | | | | |
|---|---|---|---|---|
| **Hardware (HW)** | Telèfons mòbils | Comunicació mòbil, Mobilitat dels treballadors | Alta (A) | Els telèfons mòbils són essencials per a la comunicació mòbil i la seva disponibilitat és vital per a la mobilitat dels treballadors. |
| **Hardware (HW)** | Impressores | Impressió de documents, Gestió d'equips informàtics | Alta (A) | Les impressores són importants per a la producció de documents i la seva disponibilitat és crucial per a les operacions diàries. |
| **Hardware (HW)** | Escàners | Digitalització de documents, Gestió d'equips informàtics | Alta (A) | Els escàners són essencials per a la digitalització de documents i la seva disponibilitat és vital per a la gestió de documents. |
| **Aplicacions informàtiques (SW)** | SAP | Gestió empresarial, Processos de negoci | Molt Alta (MA) | SAP és una aplicació crítica per a la gestió empresarial i la seva disponibilitat és crucial per a les operacions de la cooperativa. |
| **Aplicacions informàtiques (SW)** | Plataforma corporativa | Col·laboració interna, Comunicació interna | Molt Alta (MA) | La plataforma corporativa és fonamental per a la comunicació i la col·laboració interna, la seva disponibilitat és crucial per a les operacions. |
| **Aplicacions informàtiques (SW)** | Antivirus | Seguretat informàtica, Protecció contra amenaces | Alta (A) | L'antivirus és essencial per protegir els sistemes de la cooperativa contra amenaces de seguretat, la seva disponibilitat és crucial. |
| **Aplicacions informàtiques (SW)** | Office 365 | Col·laboració i productivitat, Correu electrònic i ofimàtica | Molt Alta (MA) | Office 365 és una suite d'aplicacions crítica per a la col·laboració i la productivitat, la seva disponibilitat és crucial per a les operacions. |
| **Suports d'informació (MED)** | Cabina d'emmagatzematge (discs durs i USB) | Emmagatzematge de dades, Seguretat de la informació | Alta (A) | La cabina d'emmagatzematge és important per a l'emmagatzematge de dades crítiques, la seva disponibilitat és crucial per a la protecció de la informació. |

| | | | | |
|---|---|---|---|---|
| **Equipament auxiliar (AUX)** | SAI | Continuïtat del negoci, Protecció contra fallades elèctriques | Alta (A) | Els SAI són importants per mantenir la continuïtat del negoci en cas de fallades elèctriques, la seva disponibilitat és crucial per a la protecció dels sistemes. |
| **Equipament auxiliar (AUX)** | Equips de climatització | Manteniment d'instal·lacions, Condicions de treball | Alta (A) | Els equips de climatització són crucials per mantenir les condicions de treball adequades, la seva disponibilitat és vital per al confort dels treballadors. |
| **Equipament auxiliar (AUX)** | Càmeres de seguretat | Seguretat física, Monitoratge de les instal·lacions | Molt Alta (MA) | Les càmeres de seguretat són essencials per a la seguretat física i el monitoratge de les instal·lacions, la seva disponibilitat és crucial per a la seguretat. |
| **Xarxes de comunicació (COM)** | Xarxa pública | Connexió a internet, Comunicacions externes | Baixa (B) | La xarxa pública és important per a la connectivitat externa, però la seva disponibilitat és menys crítica que altres actius. |
| **Xarxes de comunicació (COM)** | Xarxa privada | Comunicacions internes, Seguretat de la xarxa | Alta (A) | La xarxa privada és fonamental per a les comunicacions internes i la seguretat de la xarxa, la seva disponibilitat és crucial per a les operacions. |
| **Xarxes de comunicació (COM)** | Xarxa telefònica | Comunicació telefònica, Comunicacions internes | Molt Alta (MA) | La xarxa telefònica és crucial per a la comunicació interna i externa, la seva disponibilitat és vital per a les operacions. |
| **Instal·lacions (L)** | Planta de processament | Producció, Manteniment d'instal·lacions | Molt Alta (MA) | La planta de processament és crucial per a la producció, la seva disponibilitat és vital per a les operacions de la cooperativa. |
| **Instal·lacions (L)** | Seu central | Administració central, Operacions centrals | Molt Alta (MA) | La seu central és essencial per a l'administració i les operacions centrals de la cooperativa, la seva |

| | | | | |
|---|---|---|---|---|
| | | | | disponibilitat és vital per a les operacions. |
| **Instal·lacions (L)** | Oficina territorial | Administració regional, Operacions regionals | Alta (A) | Les oficines territorials són importants per a l'administració i les operacions regionals, la seva disponibilitat és vital per a les operacions. |
| **Persones (P)** | Treballadors | Gestió de recursos humans, Col·laboració interna | Molt Alta (MA) | Els treballadors són essencials per a la cooperativa i la seva disponibilitat és crucial per a les operacions. |
| **Persones (P)** | Administradors | Administració de sistemes, Gestió d'infraestructures | Molt Alta (MA) | Els administradors són essencials per gestionar la infraestructura i els sistemes de la cooperativa, la seva disponibilitat és crucial per a les operacions. |
| **Persones (P)** | Proveïdors | Relacions amb proveïdors, Gestió de compres | Alta (A) | Els proveïdors són importants per a l'activitat de la cooperativa. |
| **Persones (P)** | Clients | Atenció al client, Comunicació amb clients | Alta (A) | Els clients són importants per a l'activitat de la cooperativa. |

Taula 20. Dependència dels actius

### Dimensions de seguretat

Des del punt de vista de la seguretat, a més de la valoració dels actius, s'indicarà quin és l'aspecte de la seguretat més crític. Això serà de gran ajuda en el moment de pensar en possibles mesures de prevenció, ja que seran enfocades en aquells aspectes que més ens interessin.

Per tant, un cop identificats els actius, es realitzarà una valoració DICAT d'aquests (disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat). Aquesta valoració mesura la criticitat en les cinc dimensions de la seguretat de la informació vinculada al procés de negoci i ens permetrà, a posteriori, valorar l'impacte que tindrà la materialització d'una amenaça sobre la part de l'actiu exposat (no cobert per les mesures preventives a cadascuna de les dimensions).

| VALORACIÓ DELS ACTIUS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Tipus** | **Actiu** | **Valor** | **D** | **I** | **C** | **A** | **T** | **Justificació** |
| **Dades (D)** | Informació dels membres | 8,4 | 9 | 8 | 8 | 9 | 8 | Crític per a la cooperativa, inclou informació rellevant sobre membres. |
| **Dades (D)** | Dades dels clients | 8,4 | 9 | 8 | 8 | 9 | 8 | Essencial, conté informació sobre clients i transaccions. |
| **Dades (D)** | Informació financera | 8,4 | 9 | 8 | 8 | 9 | 8 | Crucial, ofereix visió de salut financera i rendiment. |
| **Dades (D)** | Registres nòmines | 7,4 | 8 | 7 | 7 | 8 | 7 | Important per a gestió del personal i conformitat legal. |
| **Dades (D)** | Còpies de seguretat | 7,6 | 7 | 8 | 8 | 7 | 8 | Essencial per a la recuperació de desastres i protecció de dades. |
| **Claus criptogràfiques (KY)** | Claus d'encriptació portàtils | 7,2 | 5 | 8 | 9 | 9 | 5 | Important per a seguretat, implementació complexa pot causar errors. |
| **Serveis (S)** | VPN | 6,4 | 7 | 5 | 5 | 9 | 6 | Important per a l'accés remot però no es crucial com a actiu. |
| **Serveis (S)** | Directori Actiu | 9,4 | 10 | 9 | 9 | 10 | 9 | Essencial per a gestió d'usuaris i autenticació, fiabilitat crucial. |
| **Serveis (S)** | Web | 7,2 | 8 | 8 | 5 | 7 | 8 | Important per a comunicació amb clients, rendiment variable. |
| **Serveis (S)** | Correu O365 | 3,8 | 4 | 4 | 4 | 3 | 4 | Útil per a la comunicació, però lluny de ser indispensable. |
| **Hardware (HW)** | Servidors | 9,4 | 10 | 9 | 9 | 10 | 9 | Crítics per a infraestructura TI, fiabilitat indispensable. |
| **Hardware (HW)** | Portàtils | 5,4 | 5 | 5 | 8 | 4 | 5 | Importants per al teletreball, però no indispensables. |
| **Hardware (HW)** | Telèfons mòbils | 7,4 | 8 | 7 | 7 | 7 | 8 | Essencials per a comunicació mòbil, disponibilitat crucial. |
| **Hardware (HW)** | Impressores | 3,6 | 4 | 2 | 4 | 4 | 4 | Importants per a impressió, però es poden prescindir. |
| **Hardware (HW)** | Escàners | 3,6 | 4 | 2 | 4 | 4 | 4 | Útils per als administradors però |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | lluny de ser essencials. |
| **Aplicacions informàtiques (SW)** | SAP | 9,4 | 10 | 9 | 9 | 10 | 9 | Crític per a processos empresarials, fiabilitat vital. |
| **Aplicacions informàtiques (SW)** | Plataforma corporativa | 9,4 | 10 | 9 | 9 | 10 | 9 | Essencial per a col·laboració interna, fiabilitat indispensable. |
| **Aplicacions informàtiques (SW)** | Antivirus | 8 | 10 | 9 | 6 | 6 | 9 | Important per a seguretat, però necessita actualitzacions regulars. |
| **Aplicacions informàtiques (SW)** | Office 365 | 8,2 | 9 | 8 | 8 | 8 | 8 | Essencial per a col·laboració i productivitat, rendiment crucial. |
| **Suports d'informació (MED)** | Cabina d'emmagatzematge (discs durs i USB) | 5 | 4 | 6 | 5 | 5 | 5 | Útil per a la cooperativa però sense gran importància. |
| **Equipament auxiliar (AUX)** | SAI | 5 | 10 | 9 | 2 | 2 | 2 | Essencial per a continuïtat del negoci, però molt momentani.. |
| **Equipament auxiliar (AUX)** | Equips de climatització | 5 | 7 | 5 | 8 | 4 | 8 | Important per a condicions de treball, però sense comprometre l'empresa. |
| **Equipament auxiliar (AUX)** | Càmeres de seguretat | 4 | 4 | 6 | 6 | 3 | 1 | Crucial per a vigilància però dispensable per a les operacions.. |
| **Xarxes de comunicació (COM)** | Xarxa pública | 7,4 | 8 | 8 | 7 | 7 | 7 | Essencial per a comunicació externa, però vulnerable a atacs. |
| **Xarxes de comunicació (COM)** | Xarxa privada | 8 | 8 | 8 | 8 | 8 | 8 | Crítica per a comunicació interna, fiabilitat indispensable. |
| **Xarxes de comunicació (COM)** | Xarxa telefònica | 8,6 | 8 | 9 | 9 | 8 | 9 | Essencial per a comunicació, fiabilitat crucial. |
| **Instal·lacions (L)** | Planta de processament | 9,3 | 10 | 9 | 9 | - | - | Crítica per a producció, fiabilitat vital. |
| **Instal·lacions (L)** | Seu central | 9,3 | 10 | 9 | 8 | - | - | Essencial per a operacions centrals, fiabilitat crucial. |
| **Instal·lacions (L)** | Oficina territorial | 8,6 | 8 | 9 | 9 | - | - | Important per a operacions regionals, fiabilitat vital. |
| **Persones (P)** | Treballadors | 6,4 | 4 | 7 | 10 | 7 | 4 | Crítics per a operacions però sense ser primordials per a totes les operacions. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Persones (P)** | Administradors | 6,4 | 4 | 7 | 10 | 7 | 4 | Crítics per a gestió de sistemes però no per a totes les operacions. |
| **Persones (P)** | Proveïdors | 6,4 | 4 | 7 | 10 | 7 | 4 | Importants per a subministrament però no per a totes les operacions. |
| **Persones (P)** | Clients | 6,4 | 4 | 7 | 10 | 7 | 4 | Crítics per a negoci però no per a totes les operacions. |

Taula 21. Valoració dels actius

## 4.2 Anàlisi d'amenaces

Els actius estan exposats a amenaces i aquestes poden afectar a diferents aspectes de la seguretat. A nivell metodològic, s'han d'analitzar quines amenaces poden afectar a quins actius a través d'un estudi, i s'ha estimar la vulnerabilitat de cada actiu respecte a les amenaces potencials, així com la freqüència estimada d'aquestes.

El més habitual en un enfocament metodològic és disposar d'una taula inicial d'amenaces. Moltes metodologies disposen de taules amb algunes de les amenaces més comunes. En aquest cas, com uso MAGERIT, es fa servir el seu llibre II "*Catálogo de Elementos*" - punt 5.

Per tant, s'ha creat aquesta taula que resumeix les amenaces que poden afectar als actius de la cooperativa agrícola i a quines dimensions (DICAT) impacta mitjançant l'escala de valors de la degradació del punt 3.5. Aquests valors son generals per a tots els actius segons el context de la cooperativa i es situen en les caselles corresponents segons a quina dimensió afectaria (extret de MAGERIT). Això no obstant, en la valoració per a cada actiu es veurà més detalladament. Els valors de la probabilitat i els seus colors pertanyen a la Taula 18. "Taula de probabilitat del punt 3.5", de manera que l'escala va d'un valor inferior (MB, verd fosc) fins a la superior (MA, roig), conservant la mateixa colorimetria com en tots els apartats amb escales.

La taula disposa de les següents amenaces segons el catàleg MAGERIT:
**[N] Desastres Naturals:** Aquestes amenaces provenen de fenòmens naturals com incendis forestals, inundacions, terratrèmols o tempestes. Són esdeveniments que poden causar danys als sistemes i instal·lacions sense intervenció humana directa.
**[I] Origen Industrial:** Aquestes amenaces sorgeixen d'activitats humanes, com fallades en equips, interrupcions en el subministrament elèctric, condicions ambientals inadequades o problemes en els serveis de comunicació. Poden ser accidents o errors derivats de processos industrials.
**[E] Errors i Fallades no Intencionades:** Aquesta categoria inclou errors causats per persones en l'ús, la configuració o la gestió de sistemes

informàtics. Poden ser des de simples errors d'usuari fins a fallades en la configuració dels equips o del programari, passant per problemes en la gestió interna de l'organització.

**[A] Atacs Intencionats:** Aquestes amenaces són resultats de l'activitat maliciosa d'individus o grups, com l'ús de credencials robades, la distribució de software maliciós, intents d'accés no autoritzat, manipulació de dades o atacs físics o virtuals als sistemes. Aquests atacs poden tenir diversos objectius, des de la obtenció d'informació confidencial fins a la interrupció de les operacions normals de l'organització.

| TAULA D'AMENACES I PROBABILITAT | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Tipus** | **Amenaça** | **Probabilitat** | **D** | **I** | **C** | **A** | **T** |
| **[N] Desastres Naturals** | N.1 Foc | MB (0,1) | 100% | - | - | - | - |
| | N.2 Danys per aigua | MB (0,1) | 75% | - | - | - | - |
| | N.9 Origen meteorològic | B (2,5) | 75% | - | - | - | - |
| **[I] Origen Industrial** | I.5 Averia d'origen físic o lògic | M (5) | 100% | - | - | - | - |
| | I.6 Tall elèctric | M (5) | 75% | - | - | - | - |
| | I.7 Condicions inadequades Temperatura o humitat | M (5) | 75% | - | - | - | - |
| | I.8 Fallada servei comunicacions | M (5) | 100% | - | - | - | - |
| | I.9 Interrupció d'altres serveis | B (2,5) | 100% | - | - | - | - |
| | I.10 Degradació dels suports d'emmagatzematge | B (2,5) | 75% | - | - | - | - |
| **[E] Errors i fallades no intencionades** | E.1 Errors d'usuaris | MA (10) | 75% | 50% | 50% | - | - |
| | E.2 Errors d'administrador | M (5) | 75% | 50% | 50% | - | - |
| | E.3 Errors de monitorització | M (5) | - | 50% | - | - | 50% |
| | E.4 Errors de configuració | M (5) | - | 50% | - | - | - |
| | E.7 Deficiències amb la organització | M (5) | 50% | - | - | - | - |
| | E.8 Difusió de software maligne | M (5) | 100% | 50% | 50% | - | - |
| | E.10 Errors de seqüència | B (2,5) | - | 25% | - | - | - |
| | E.15 Alteració accidental de la informació | A (7,5) | 25% | 100% | - | - | - |
| | E.18 Destrucció de la informació | A (7,5) | 100% | - | - | - | - |
| | E.19 Fuga de informació | M (5) | - | - | 100% | - | - |
| | E.20 Vulnerabilitat dels programes | A (7,5) | 75% | 75% | 75% | - | - |
| | E.21 Errors manteniment o actualització de programes | M (5) | 75% | 50% | - | - | - |
| | E.23 Errors manteniment o actualització d'equips | M (5) | 75% | - | - | - | - |
| | E.24 Caiguda de sistema per esgotament de recursos | M (5) | 100% | - | - | - | - |
| | E.25 Pèrdua d'equips | M (5) | 100% | - | 25% | - | - |
| | E.28 Indisponiblitat del personal | M (5) | 75% | - | - | - | - |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **[A] Atacs intencionats** | A.3 Manipulació dels registres d'activitat (log) | M (5) | - | 75% | - | - | 25% |
| | A.4 Manipulació de la informació | A (7,5) | 75% | 75% | 75% | - | - |
| | A.5 Suplantació d'identitat | A (7,5) | - | 75% | 100% | 100% | - |
| | A.6 Abús de privilegis d'accés | M (5) | 25% | 75% | 75% | - | - |
| | A.7 Ús no previst | MA (10) | 75% | 75% | 75% | - | - |
| | A.8 Difusió de software maligne | A (7,5) | 75% | 75% | 75% | - | - |
| | A.11 Accés no autoritzat | M (5) | - | 100% | 75% | - | - |
| | A.15 Modificació deliberada de la informació | M (5) | - | 100% | - | - | - |
| | A.18 Destrucció de la informació | A (7,5) | 100% | - | - | - | - |
| | A.19 Divulgació de informació | M (5) | - | - | 75% | - | - |
| | A.22 Manipulació de programes | M (5) | 75% | 75% | 75% | - | - |
| | A.22 Manipulació dels equips | A (7,5) | 75% | - | 75% | - | - |
| | A.24 Denegació de servei | M (5) | 100% | - | - | - | - |
| | A.25 Robatori | M (5) | 25% | - | 100% | - | - |
| | A.26 Atac destructiu | B (2,5) | 100% | - | - | - | - |
| | A.28 Indisponiblitat del personal | M (5) | 75% | - | - | - | - |
| | A.29 Extorsió | B (2,5) | 75% | 75% | 75% | - | - |
| | A.30 Enginyeria social | B (2,5) | 75% | 75% | 75% | - | - |

Taula 22. Amenaces i probabilitat

**Resum de la taula:**

Respecte a la probabilitat, les amenaces de tipus desastre natural són les menys probables, amb una classificació de MB (Molt Baixa) de mitja 0,9. Les següents en ordre de probabilitat són les d'origen industrial, amb una classificació de B (Baixa) gairebé M (Mitjana) amb mitja de 4,16. Seguint a aquestes, trobem les dues més probables que ocorrin: els atacs intencionats, classificats com a M (Mitjana) amb un percentatge de 5,88 i els errors humans, també classificats com a M (Mitjana) amb mitja de 5,625.

En general, les amenaces tenen un impacte molt significatiu en la Disponibilitat, ja que la majoria d'elles afecten aquesta dimensió i amb una alta degradació (normalment del 75%). Això és especialment evident en les amenaces de tipus desastre natural (N) i d'origen industrial (I), on només es veu compromesa la Disponibilitat.

En canvi, les amenaces dels tipus Errors (E) i Atacs (A) també poden impactar en altres dimensions, encara que la Disponibilitat encara és la més afectada. Però també hi ha d'afectades en Integritat i Confidencialitat, amb només una amenaça impactant en l'Autenticitat i dues en la Traçabilitat.

### 4.3 Valoració del l'impacte, risc i accions

Un cop ben identificats els actius, s'identifica l'impacte que poden provocar les diferents amenaces.
Recordem que els valors i les fórmules d'aquesta taula estan en el punt 3.6. Això no obstant, recordem els aspectes més importants per a una major lectura.

**Risc inicial (o potencial):** S'anomena risc a la mida del dany probable sobre un sistema. Coneixent l'impacte de les amenaces sobre els actius, és directe derivar el risc només tenint en compte la probabilitat d'ocurrència. Per tant, és el risc en el que està exposada la cooperativa tenint en compte les mesures de seguretat del moment.

La mitigació de riscos és el procés de reduir amenaces o riscos potencials a què s'exposa la cooperativa com a projecte, i consisteix a identificar els riscos i desenvolupar un pla per gestionar-los o eliminar-los; de manera que es pugui continuar avançant amb confiança, sense importar la dificultat del que cal resoldre.

Les quatre estratègies per a la mitigació dels riscos que faig servir és:

- Evitar
- Mitigar
- Derivar
- Assumir

**Nivell de risc acceptable**: La cooperativa té com ombrall de risc acceptable el valor de 15. Això significa que si es igual o menor a aquest valor, s'assumirà el risc. Però si es més gran s'haurà de mitigar, reduir o eliminar.

**Risc residual:** És el risc resultant després d'aplicar els plans de tractament i mitigar els riscos que no són acceptables.

Com les amenaces que superen el límit definit de 15 suposen una amenaça important per a la cooperativa, s'apliquen les estratègies mencionades que funcionen com a controls establerts per a **reduir el risc inicial** i passar-lo a un **risc residual**. Aquest, continuarà existint, però el desitjable és aconseguir reduir-lo per tal que estigui per sota del nivell acceptable.

Per tant, un cop aplicats els controls ISO/IEC 27001:2023 i executades les accions de tractament de risc, és calcula que tindran una reducció percentual del 70% del valor total (x0,3), perquè en ser una cooperativa que disposa d'ajudes econòmiques i d'alt valor, comptaria amb el pressupost adequat per a cobrir les accions requerides. De nou, repetir que les que estiguin per sota del risc acceptable, passaran a ser assumibles i no s'haurà d'efectuar cap control.

| 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 | Errors d'usuaris | 5 | 25% | 2,1 | 10,5 | Assumir | - |
| | | E.2 | Errors 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 |
| **(D) Dades dels clients** | 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 | Errors d'usuaris | 5 | 25% | 2,1 | 10,5 | Assumir | - |
| | | E.2 | Errors d'administrador | 5 | 50% | 4,2 | 21 | **Mitigar** | 6,3 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 25% | 2,1 | 15,75 | Assumir | - |
| | | E.18 | Destrucció de la informació | 7,5 | 50% | 4,2 | 31,5 | **Mitigar** | 9,45 |
| | | E.19 | Fuga de informació | 10 | 50% | 4,2 | 42 | **Evitar** | 12,6 |
| | | A.4 | Manipulació de la informació | 5 | 30% | 2,52 | 12,6 | Assumir | - |
| | | A.5 | Suplantació d'identitat | 7,5 | 40% | 3,36 | 25,2 | **Mitigar** | 7,56 |
| | | A.6 | Abús de privilegis d'accés | 5 | 20% | 1,68 | 8,4 | Assumir | - |
| | | A.11 | Accés no autoritzat | 5 | 30% | 2,52 | 12,6 | Assumir | - |
| | | A.15 | Modificació deliberada de la informació | 5 | 30% | 2,52 | 12,6 | Assumir | - |
| | | A.18 | Destrucció de la informació | 7,5 | 70% | 5,88 | 44,1 | **Evitar** | 13,23 |
| | | A.19 | Divulgació de informació | 5 | 25% | 2,1 | 10,5 | Assumir | - |
| **(D) Informació financera** | 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 | Errors d'usuaris | 10 | 50% | 4,2 | 42 | **Mitigar** | 12,6 |
| | | E.2 | Errors 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 | 5 | 25% | 1,85 | 9,25 | Assumir | - |
| | | E.19 | Fuga de informació | 7,5 | 75% | 5,55 | 41,625 | **Evitar** | 12,4875 |
| | | 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 | **Mitigar** | 0,252 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 6,3 | 31,5 | **Mitigar** | 0,189 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 6,3 | 31,5 | **Evitar** | 3,15 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 6,3 | 31,5 | **Mitigar** | 6,3 |
| | | A.18 | Destrucció de la informació | 7,5 | 100% | 8,4 | 63 | **Mitigar** | 9,45 |
| | | A.19 | Divulgació de informació | 5 | 100% | 8,4 | 42 | **Mitigar** | 14,175 |
| **(D) Registres nòmines** | 7,4 | N.1 | Foc | 0,1 | 100% | 7,4 | 0,74 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 75% | 5,55 | 0,555 | Assumir | - |
| | | E.1 | Errors d'usuaris | 10 | 50% | 3,7 | 37 | **Mitigar** | 14,175 |
| | | E.2 | Errors d'administrador | 5 | 50% | 3,7 | 18,5 | **Mitigar** | 9,45 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 3,7 | 27,75 | **Mitigar** | 9,45 |
| | | E.18 | Destrucció de la informació | 5 | 25% | 1,85 | 9,25 | Assumir | - |
| | | E.19 | Fuga de informació | 7,5 | 75% | 5,55 | 41,625 | **Evitar** | 18,9 |
| | | A.4 | Manipulació de la informació | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 9,45 |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 5,55 | 41,625 | **Mitigar** | 0,252 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 0,189 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 3,15 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 6,3 |
| | | A.18 | Destrucció de la informació | 7,5 | 100% | 7,4 | 55,5 | **Evitar** | 4,725 |
| | | A.19 | Divulgació de informació | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 9,45 |
| **(D) Còpies de seguretat** | 7,4 | N.1 | Foc | 0,1 | 100% | 7,4 | 0,74 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 75% | 5,55 | 0,555 | Assumir | - |
| | | E.1 | Errors d'usuaris | 10 | 50% | 3,7 | 37 | **Mitigar** | 7,56 |
| | | E.2 | Errors d'administrador | 5 | 50% | 3,7 | 18,5 | **Mitigar** | 2,52 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 3,7 | 27,75 | **Mitigar** | 3,78 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 5,55 | 41,625 | **Evitar** | 3,78 |
| | | E.19 | Fuga de informació | 7,5 | 75% | 5,55 | 41,625 | **Evitar** | 13,23 |
| | | A.4 | Manipulació de la informació | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 3,15 |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 5,55 | 41,625 | **Mitigar** | 0,252 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 0,189 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 12,6 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 6,3 |
| | | A.18 | Destrucció de la informació | 7,5 | 100% | 7,4 | 55,5 | **Mitigar** | 9,45 |
| | | A.19 | Divulgació de informació | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 2,775 |

Taula 23. Anàlisi de risc Dades (D)

| Actiu | Valor | Amenaça | | Prob | Degradació | Impacte | Risc inicial | Acció | Risc residual |
|---|---|---|---|---|---|---|---|---|---|
| **(KY) Claus Criptogràfiques** | 7,2 | E.1 | Errors d'usuaris | 10 | 25% | 1,8 | 18 | **Mitigar** | 5,4 |
| | | E.2 | Errors d'administrador | 5 | 25% | 1,8 | 9 | Assumir | - |
| | | E.15 | Alteració accidental de la informació | 7,5 | 25% | 1,8 | 13,5 | Assumir | - |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | E.18 | Destrucció de la informació | 7,5 | 25% | 1,8 | 13,5 | Assumir | - |
| | | E.19 | Fuga de informació | 5 | 25% | 1,8 | 9 | Assumir | - |
| | | A.5 | Suplantació d'identitat | 7,5 | 25% | 1,8 | 13,5 | Assumir | - |
| | | A.6 | Abús de privilegis d'accés | 5 | 25% | 1,8 | 9 | Assumir | - |
| | | A.11 | Accés no autoritzat | 5 | 25% | 1,8 | 9 | Assumir | - |
| | | A.15 | Modificació deliberada de la informació | 5 | 25% | 1,8 | 9 | Assumir | - |
| | | A.18 | Destrucció de la informació | 7,5 | 25% | 1,8 | 13,5 | Assumir | - |
| | | A.19 | Divulgació de informació | 5 | 25% | 1,8 | 9 | Assumir | - |

Taula 24. Anàlisi de risc Claus Criptogràfiques (KY)

| Actiu | Valor | Amenaça | | Prob | Degradació | Impacte | Risc inicial | Acció | Risc residual |
|---|---|---|---|---|---|---|---|---|---|
| **(S) VPN** | 6,4 | E.1 | Errors d'usuaris | 10 | 75% | 4,8 | 48 | **Mitigar** | 14,4 |
| | | E.2 | Errors d'administrador | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 3,2 | 24 | **Mitigar** | 7,2 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 4,8 | 36 | **Mitigar** | 10,8 |
| | | E.19 | Fuga de informació | 5 | 25% | 1,6 | 8 | Assumir | - |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 50% | 3,2 | 16 | Assumir | - |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 4,8 | 36 | **Mitigar** | 10,8 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | A.7 | Ús no previst | 10 | 75% | 4,8 | 48 | **Mitigar** | 14,4 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | A.18 | Destrucció de la informació | 7,5 | 75% | 4,8 | 36 | **Mitigar** | 10,8 |
| | | A.19 | Divulgació de informació | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | A.24 | Denegació de servei | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| **(S) Directori Actiu** | 9,4 | E.1 | Errors d'usuaris | 10 | 75% | 7,05 | 70,5 | **Mitigar** | 21,15 |
| | | E.2 | Errors d'administrador | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 4,7 | 35,25 | **Mitigar** | 10,575 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | E.19 | Fuga de informació | 5 | 25% | 2,35 | 11,75 | Assumir | - |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 50% | 4,7 | 23,5 | **Mitigar** | 7,05 |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.7 | Ús no previst | 10 | 75% | 7,05 | 70,5 | **Mitigar** | 21,15 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.18 | Destrucció de la informació | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | A.19 | Divulgació de informació | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | A.24 | Denegació de servei | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| **(S) Web** | 7,2 | E.1 | Errors d'usuaris | 10 | 75% | 5,4 | 54 | **Mitigar** | 16,2 |
| | | E.2 | Errors d'administrador | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 3,6 | 27 | **Mitigar** | 8,1 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 5,4 | 40,5 | **Mitigar** | 12,15 |
| | | E.19 | Fuga de informació | 5 | 25% | 1,8 | 9 | Assumir | - |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 50% | 3,6 | 18 | **Mitigar** | 5,4 |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 5,4 | 40,5 | **Mitigar** | 12,15 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | A.7 | Ús no previst | 10 | 75% | 5,4 | 54 | **Mitigar** | 16,2 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | A.18 | Destrucció de la informació | 7,5 | 75% | 5,4 | 40,5 | **Mitigar** | 12,15 |
| | | A.19 | Divulgació de informació | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | A.24 | Denegació de servei | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| **(S) Correu O365** | 3,8 | E.1 | Errors d'usuaris | 10 | 75% | 2,85 | 28,5 | **Mitigar** | 8,55 |
| | | E.2 | Errors d'administrador | 5 | 75% | 2,85 | 14,25 | Assumir | - |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 1,9 | 14,25 | Assumir | - |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 2,85 | 21,375 | **Mitigar** | 6,4125 |
| | | E.19 | Fuga de informació | 5 | 25% | 0,95 | 4,75 | Assumir | - |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 50% | 1,9 | 9,5 | Assumir | - |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 75% | 2,85 | 14,25 | Assumir | - |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 2,85 | 21,375 | **Mitigar** | 6,4125 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 2,85 | 14,25 | Assumir | - |
| | | A.7 | Ús no previst | 10 | 75% | 2,85 | 28,5 | **Mitigar** | 8,55 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 2,85 | 14,25 | Assumir | - |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 2,85 | 14,25 | Assumir | - |
| | | A.18 | Destrucció de la informació | 7,5 | 75% | 2,85 | 21,375 | **Mitigar** | 6,4125 |
| | | A.19 | Divulgació de informació | 5 | 75% | 2,85 | 14,25 | Assumir | - |
| | | A.24 | Denegació de servei | 5 | 75% | 2,85 | 14,25 | Assumir | - |

Taula 25. Anàlisi de risc Serveis (S)

| Actiu | Valor | Amenaça | | Prob | Degradació | Impacte | Risc inicial | Acció | Risc residual |
|---|---|---|---|---|---|---|---|---|---|
| **(HW) Servidors** | 9,4 | N.1 | Foc | 0,1 | 75% | 7,05 | 0,705 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 50% | 4,7 | 0,47 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 50% | 4,7 | 11,75 | Assumir | - |
| | | I.5 | Averia d'origen físic o lògic | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | I.6 | Tall elèctric | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | I.7 | Condicions inadequades Temperatura o humitat | 5 | 50% | 4,7 | 23,5 | **Mitigar** | 7,05 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | E.2 | Erros d'administrador | 5 | 50% | 4,7 | 23,5 | **Mitigar** | 7,05 |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 50% | 4,7 | 23,5 | **Mitigar** | 7,05 |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | E.25 | Pèrdua d'equips | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.7 | Ús no previst | 10 | 75% | 7,05 | 70,5 | **Evitar** | 21,15 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.25 | Robatori | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| **(HW) Portàtils** | 5,4 | N.1 | Foc | 0,1 | 50% | 2,7 | 0,27 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 25% | 1,35 | 0,135 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 25% | 1,35 | 3,375 | Assumir | - |
| | | I.5 | Averia d'origen físic o lògic | 5 | 50% | 2,7 | 13,5 | Assumir | - |
| | | I.6 | Tall elèctric | 5 | 50% | 2,7 | 13,5 | Assumir | - |
| | | I.7 | Condicions inadequades Temperatura o humitat | 5 | 25% | 1,35 | 6,75 | Assumir | - |
| | | E.2 | Erros d'administrador | 5 | 25% | 1,35 | 6,75 | Assumir | - |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 25% | 1,35 | 6,75 | Assumir | - |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 50% | 2,7 | 13,5 | Assumir | - |
| | | E.25 | Pèrdua d'equips | 5 | 50% | 2,7 | 13,5 | Assumir | - |
| | | A.6 | Abús de privilegis d'accés | 5 | 50% | 2,7 | 13,5 | Assumir | - |
| | | A.7 | Ús no previst | 10 | 50% | 2,7 | 27 | **Mitigar** | 8,1 |
| | | A.11 | Accés no autoritzat | 5 | 50% | 2,7 | 13,5 | Assumir | - |
| | | A.25 | Robatori | 5 | 50% | 2,7 | 13,5 | Assumir | - |
| **(HW) Telèfons mòbils** | 7,4 | N.1 | Foc | 0,1 | 75% | 5,55 | 0,555 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 50% | 3,7 | 0,37 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 50% | 3,7 | 9,25 | Assumir | - |
| | | I.5 | Averia d'origen físic o lògic | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 8,325 |
| | | I.6 | Tall elèctric | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 8,325 |
| | | I.7 | Condicions inadequades Temperatura o humitat | 5 | 50% | 3,7 | 18,5 | **Mitigar** | 5,55 |
| | | E.2 | Erros d'administrador | 5 | 50% | 3,7 | 18,5 | **Mitigar** | 5,55 |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 50% | 3,7 | 18,5 | **Mitigar** | 5,55 |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 8,325 |
| | | E.25 | Pèrdua d'equips | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 8,325 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 8,325 |
| | | A.7 | Ús no previst | 10 | 75% | 5,55 | 55,5 | **Mitigar** | 16,65 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 8,325 |
| | | A.25 | Robatori | 5 | 75% | 5,55 | 27,75 | **Mitigar** | 8,325 |
| **(HW) Impressores** | 3,6 | N.1 | Foc | 0,1 | 100% | 3,6 | 0,09 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 100% | 3,6 | 0,36 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 0% | 0 | 0 | Assumir | - |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | I.5 | Averia d'origen físic o lògic | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | I.6 | Tall elèctric | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | I.7 | Condicions inadequades Temperatura o humitat | 5 | 50% | 1,8 | 9 | Assumir | - |
| | | E.2 | Errors d'administrador | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | E.25 | Pèrdua d'equips | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | A.6 | Abús de privilegis d'accés | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | A.7 | Ús no previst | 10 | 25% | 0,9 | 9 | Assumir | - |
| | | A.11 | Accés no autoritzat | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | A.25 | Robatori | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| **(HW) Escàners** | 3,6 | N.1 | Foc | 0,1 | 100% | 3,6 | 0,36 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 100% | 3,6 | 0,36 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 0% | 0 | 0 | Assumir | - |
| | | I.5 | Averia d'origen físic o lògic | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | I.6 | Tall elèctric | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | I.7 | Condicions inadequades Temperatura o humitat | 5 | 50% | 1,8 | 9 | Assumir | - |
| | | E.2 | Errors d'administrador | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | E.25 | Pèrdua d'equips | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | A.6 | Abús de privilegis d'accés | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | A.7 | Ús no previst | 10 | 25% | 0,9 | 9 | Assumir | - |
| | | A.11 | Accés no autoritzat | 5 | 25% | 0,9 | 4,5 | Assumir | - |
| | | A.25 | Robatori | 5 | 25% | 0,9 | 4,5 | Assumir | - |

Taula 26. Anàlisi de risc Hardware (HW)

| Actiu | Valor | Amenaça | | Prob | Degradació | Impacte | Risc inicial | Acció | Risc residual |
|---|---|---|---|---|---|---|---|---|---|
| **(SW) SAP** | 9,4 | I.5 | Averia d'origen físic o lògic | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | E.1 | Errors d'usuaris | 10 | 50% | 4,7 | 47 | **Mitigar** | 14,1 |
| | | E.2 | Errors d'administrador | 5 | 50% | 4,7 | 23,5 | **Mitigar** | 7,05 |
| | | E.8 | Difusió de software maligne | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 4,7 | 35,25 | **Mitigar** | 10,575 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | E.19 | Fuga de informació | 5 | 25% | 2,35 | 11,75 | Assumir | - |
| | | E.20 | Vulnerabilitat dels programes | 7,5 | 50% | 4,7 | 35,25 | **Mitigar** | 10,575 |
| | | E.21 | Errors manteniment o actualització de programes | 5 | 50% | 4,7 | 23,5 | **Mitigar** | 7,05 |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | A.7 | Ús no previst | 10 | 50% | 4,7 | 47 | **Mitigar** | 14,1 |
| | | A.8 | Difusió de software maligne | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 7,05 | 35,25 | **Evitar** | 10,575 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.18 | Destrucció de la informació | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | A.19 | Divulgació de informació | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| **(SW) Plataforma corporativa** | 9,4 | I.5 | Averia d'origen físic o lògic | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | E.1 | Errors d'usuaris | 10 | 50% | 4,7 | 47 | **Mitigar** | 14,1 |
| | | E.2 | Errors d'administrador | 5 | 50% | 4,7 | 23,5 | **Mitigar** | 7,05 |
| | | E.8 | Difusió de software maligne | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 4,7 | 35,25 | **Mitigar** | 10,575 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | E.19 | Fuga de informació | 7,5 | 75% | 7,05 | 52,875 | **Evitar** | 15,8625 |
| | | E.20 | Vulnerabilitat dels programes | 7,5 | 50% | 4,7 | 35,25 | **Mitigar** | 10,575 |
| | | E.21 | Errors manteniment o actualització de programes | 5 | 50% | 4,7 | 23,5 | **Mitigar** | 7,05 |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.7 | Ús no previst | 10 | 50% | 4,7 | 47 | **Mitigar** | 14,1 |
| | | A.8 | Difusió de software maligne | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 7,05 | 35,25 | **Evitar** | 10,575 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| | | A.18 | Destrucció de la informació | 7,5 | 75% | 7,05 | 52,875 | **Mitigar** | 15,8625 |
| | | A.19 | Divulgació de informació | 5 | 75% | 7,05 | 35,25 | **Mitigar** | 10,575 |
| **(SW) Antivirus** | 8 | I.5 | Averia d'origen físic o lògic | 5 | 75% | 6 | 30 | **Derivar** | 9 |
| | | E.1 | Errors d'usuaris | 10 | 50% | 4 | 40 | **Mitigar** | 12 |
| | | E.2 | Errors d'administrador | 5 | 50% | 4 | 20 | **Mitigar** | 6 |
| | | E.8 | Difusió de software maligne | 5 | 75% | 6 | 30 | **Derivar** | 9 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 4 | 30 | **Derivar** | 9 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 6 | 45 | **Derivar** | 13,5 |
| | | E.19 | Fuga de informació | 5 | 25% | 2 | 10 | Assumir | - |
| | | E.20 | Vulnerabilitat dels programes | 7,5 | 50% | 4 | 30 | **Derivar** | 9 |
| | | E.21 | Errors manteniment o actualització de programes | 5 | 50% | 4 | 20 | **Derivar** | 6 |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 6 | 45 | **Derivar** | 13,5 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 6 | 30 | **Derivar** | 9 |
| | | A.7 | Ús no previst | 10 | 50% | 4 | 40 | **Derivar** | 12 |
| | | A.8 | Difusió de software maligne | 7,5 | 75% | 6 | 45 | **Derivar** | 13,5 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 6 | 30 | **Derivar** | 9 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 6 | 30 | **Derivar** | 9 |
| | | A.18 | Destrucció de la informació | 7,5 | 75% | 6 | 45 | **Derivar** | 13,5 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | A.19 | Divulgació de informació | 5 | 75% | 6 | 30 | **Derivar** | 9 |
| **(SW) Office 365** | 8,2 | I.5 | Averia d'origen físic o lògic | 5 | 75% | 6,15 | 30,75 | **Mitigar** | 9,225 |
| | | E.1 | Errors d'usuaris | 10 | 50% | 4,1 | 41 | **Mitigar** | 12,3 |
| | | E.2 | Errors d'administrador | 5 | 50% | 4,1 | 20,5 | **Mitigar** | 6,15 |
| | | E.8 | Difusió de software maligne | 5 | 75% | 6,15 | 30,75 | **Mitigar** | 9,225 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 4,1 | 30,75 | **Mitigar** | 9,225 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 6,15 | 46,125 | **Mitigar** | 13,8375 |
| | | E.19 | Fuga de informació | 5 | 25% | 2,05 | 10,25 | Assumir | - |
| | | E.20 | Vulnerabilitat dels programes | 7,5 | 50% | 4,1 | 30,75 | **Mitigar** | 9,225 |
| | | E.21 | Errors manteniment o actualització de programes | 5 | 50% | 4,1 | 20,5 | **Mitigar** | 6,15 |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 6,15 | 46,125 | **Mitigar** | 13,8375 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 6,15 | 30,75 | **Mitigar** | 9,225 |
| | | A.7 | Ús no previst | 10 | 50% | 4,1 | 41 | **Mitigar** | 12,3 |
| | | A.8 | Difusió de software maligne | 7,5 | 75% | 6,15 | 46,125 | **Mitigar** | 13,8375 |
| | | A.11 | Accés no autoritzat | 5 | 75% | 6,15 | 30,75 | **Mitigar** | 9,225 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 6,15 | 30,75 | **Mitigar** | 9,225 |
| | | A.18 | Destrucció de la informació | 7,5 | 75% | 6,15 | 46,125 | **Mitigar** | 13,8375 |
| | | A.19 | Divulgació de informació | 5 | 75% | 6,15 | 30,75 | **Mitigar** | 9,225 |

Taula 26. Anàlisi de risc Software (SW)

| Actiu | Valor | Amenaça | | Prob | Degradació | Impacte | Risc inicial | Acció | Risc residual |
|---|---|---|---|---|---|---|---|---|---|
| **(MED) Cabina d'emmagatematge** | 5 | N.1 | Foc | 0,1 | 75% | 3,75 | 0,375 | Assumir | - |
| | | N.2 | Danys per aigua | 2,5 | 50% | 2,5 | 6,25 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 75% | 3,75 | 9,375 | Assumir | - |
| | | I.5 | Averia d'origen físic o lògic | 7,5 | 75% | 3,75 | 28,125 | **Mitigar** | 8,4375 |
| | | I.6 | Tall elèctric | 5 | 25% | 1,25 | 6,25 | Assumir | - |
| | | I.7 | Condicions inadequades Temperatura o humitat | 7,5 | 75% | 3,75 | 28,125 | **Mitigar** | 8,4375 |
| | | I.10 | Degradació dels suports d'emmagatzematge | 2,5 | 50% | 2,5 | 6,25 | Assumir | - |
| | | E.1 | Errors d'usuaris | 10 | 75% | 3,75 | 37,5 | **Mitigar** | 11,25 |
| | | E.2 | Erros d'administrador | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | E.15 | Alteració accidental de la informació | 7,5 | 75% | 3,75 | 28,125 | **Mitigar** | 8,4375 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 3,75 | 28,125 | **Mitigar** | 8,4375 |
| | | E.19 | Fuga de informació | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | E.25 | Pèrdua d'equips | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | A.7 | Ús no previst | 10 | 75% | 3,75 | 37,5 | **Mitigar** | 11,25 |

Taula 27. Anàlisi de risc Suports d'Informació (MED)

| Actiu | Valor | Amenaça | | Prob | Degradació | Impacte | Risc inicial | Acció | Risc residual |
|---|---|---|---|---|---|---|---|---|---|
| **(AUX) SAI** | 5 | N.1 | Foc | 0,1 | 50% | 2,5 | 0,25 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 50% | 2,5 | 0,25 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 50% | 2,5 | 6,25 | Assumir | - |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | I.5 | Averia d'origen físic o lògic | 7,5 | 50% | 2,5 | 18,75 | **Mitigar** | 5,625 |
| | | I.6 | Tall elèctric | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | I.7 | Condicions inadequades Temperatura o humitat | 7,5 | 50% | 2,5 | 18,75 | **Mitigar** | 5,625 |
| | | I.9 | Interrupció d'altres serveis | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | E.25 | Pèrdua d'equips | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | A.7 | Ús no previst | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | A.11 | Accés no autoritzat | 7,5 | 50% | 2,5 | 18,75 | **Mitigar** | 5,625 |
| | | A.25 | Robatori | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| **(AUX) Equips de climatitzaci ó** | 5 | N.1 | Foc | 0,1 | 50% | 2,5 | 0,25 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 50% | 2,5 | 0,25 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 50% | 2,5 | 6,25 | Assumir | - |
| | | I.5 | Averia d'origen físic o lògic | 7,5 | 75% | 3,75 | 28,125 | **Mitigar** | 8,4375 |
| | | I.6 | Tall elèctric | 5 | 25% | 1,25 | 6,25 | Assumir | - |
| | | I.7 | Condicions inadequades Temperatura o humitat | 7,5 | 75% | 3,75 | 28,125 | **Mitigar** | 8,4375 |
| | | I.9 | Interrupció d'altres serveis | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | E.25 | Pèrdua d'equips | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | A.7 | Ús no previst | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | A.11 | Accés no autoritzat | 7,5 | 75% | 3,75 | 28,125 | **Evitar** | 8,4375 |
| | | A.25 | Robatori | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| **(AUX) Càmeres de seguretat** | 5 | N.1 | Foc | 0,1 | 50% | 2,5 | 0,25 | Assumir | - |
| | | N.2 | Danys per aigua | 0,1 | 50% | 2,5 | 0,25 | Assumir | - |
| | | N.9 | Origen meteorològic | 0,25 | 50% | 2,5 | 0,625 | Assumir | - |
| | | I.5 | Averia d'origen físic o lògic | 7,5 | 75% | 3,75 | 28,125 | **Mitigar** | 8,4375 |
| | | I.6 | Tall elèctric | 5 | 25% | 1,25 | 6,25 | Assumir | - |
| | | I.7 | Condicions inadequades Temperatura o humitat | 5 | 50% | 2,5 | 12,5 | Assumir | - |
| | | I.9 | Interrupció d'altres serveis | 5 | 75% | 3,75 | 18,75 | **Mitigar** | 5,625 |
| | | E.25 | Pèrdua d'equips | 5 | 75% | 3,75 | 18,75 | **Mitigar** | 5,625 |
| | | A.7 | Ús no previst | 5 | 75% | 3,75 | 18,75 | **Mitigar** | 5,625 |
| | | A.11 | Accés no autoritzat | 7,5 | 100% | 5 | 37,5 | **Mitigar** | 11,25 |
| | | A.25 | Robatori | 2,5 | 75% | 3,75 | 9,375 | Assumir | - |

Taula 28. Anàlisi de risc Equipament Auxiliar (AUX)

| Actiu | Valor | Amenaça | | Prob | Degradació | Impacte | Risc inicial | Acció | Risc residual |
|---|---|---|---|---|---|---|---|---|---|
| **(COM) Xarxa Pública** | 7,2 | I.8 | Fallada servei comunicacions | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | E.2 | Errors d'administrador | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 3,6 | 27 | **Mitigar** | 8,1 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 5,4 | 40,5 | **Mitigar** | 12,15 |
| | | E.19 | Fuga de informació | 5 | 50% | 3,6 | 18 | **Mitigar** | 5,4 |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | E.24 | Caiguda de sistema per esgotament de | 5 | 25% | 1,8 | 9 | Assumir | - |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | recursos | | | | | | |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 5,4 | 40,5 | **Evitar** | 12,15 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | A.7 | Ús no previst | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | A.11 | Accés no autoritzat | 7,5 | 100% | 7,2 | 54 | **Mitigar** | 16,2 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | A.19 | Divulgació de informació | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| | | A.24 | Denegació de servei | 5 | 75% | 5,4 | 27 | **Mitigar** | 8,1 |
| **(COM) Xarxa Privada** | 8 | I.8 | Fallada servei comunicacions | 5 | 75% | 6 | 30 | **Mitigar** | 9 |
| | | E.2 | Errors d'administrador | 5 | 75% | 6 | 30 | **Mitigar** | 9 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 4 | 30 | **Mitigar** | 9 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 6 | 45 | **Mitigar** | 13,5 |
| | | E.19 | Fuga de informació | 5 | 50% | 4 | 20 | **Mitigar** | 6 |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 75% | 6 | 30 | **Mitigar** | 9 |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 25% | 2 | 10 | Assumir | - |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 6 | 45 | **Evitar** | 13,5 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 6 | 30 | **Mitigar** | 9 |
| | | A.7 | Ús no previst | 5 | 75% | 6 | 30 | **Mitigar** | 9 |
| | | A.11 | Accés no autoritzat | 7,5 | 100% | 8 | 60 | **Evitar** | 18 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 6 | 30 | **Mitigar** | 9 |
| | | A.19 | Divulgació de informació | 5 | 75% | 6 | 30 | **Mitigar** | 9 |
| | | A.24 | Denegació de servei | 5 | 75% | 6 | 30 | **Mitigar** | 9 |
| **(COM) Xarxa Telefònica** | 8,6 | I.8 | Fallada servei comunicacions | 5 | 75% | 6,45 | 32,25 | **Mitigar** | 9,675 |
| | | E.2 | Errors d'administrador | 5 | 75% | 6,45 | 32,25 | **Mitigar** | 9,675 |
| | | E.15 | Alteració accidental de la informació | 7,5 | 50% | 4,3 | 32,25 | **Mitigar** | 9,675 |
| | | E.18 | Destrucció de la informació | 7,5 | 75% | 6,45 | 48,375 | **Mitigar** | 14,5125 |
| | | E.19 | Fuga de informació | 5 | 50% | 4,3 | 21,5 | **Mitigar** | 6,45 |
| | | E.23 | Errors manteniment o actualització d'equips | 5 | 75% | 6,45 | 32,25 | **Mitigar** | 9,675 |
| | | E.24 | Caiguda de sistema per esgotament de recursos | 5 | 25% | 2,15 | 10,75 | Assumir | - |
| | | A.5 | Suplantació d'identitat | 7,5 | 75% | 6,45 | 48,375 | **Mitigar** | 14,5125 |
| | | A.6 | Abús de privilegis d'accés | 5 | 75% | 6,45 | 32,25 | **Mitigar** | 9,675 |
| | | A.7 | Ús no previst | 5 | 75% | 6,45 | 32,25 | **Mitigar** | 9,675 |
| | | A.11 | Accés no autoritzat | 7,5 | 100% | 8,6 | 64,5 | **Evitar** | 19,35 |
| | | A.15 | Modificació deliberada de la informació | 5 | 75% | 6,45 | 32,25 | **Mitigar** | 9,675 |
| | | A.19 | Divulgació de informació | 5 | 75% | 6,45 | 32,25 | **Mitigar** | 9,675 |
| | | A.24 | Denegació de servei | 5 | 75% | 6,45 | 32,25 | **Mitigar** | 9,675 |

Taula 29. Anàlisi de risc Xarxes de Comunicació (COM)

| Actiu | Valor | Amenaça | | Prob | Degradació | Impacte | Risc inicial | Acció | Risc residual |
|---|---|---|---|---|---|---|---|---|---|
| **(L) Planta** | 9,3 | N.1 | Foc | 0,1 | 100% | 9,3 | 0,93 | Assumir | - |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **de processament** | | N.2 | Danys per aigua | 2,5 | 75% | 6,975 | 17,437 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 50% | 4,65 | 11,625 | Assumir | - |
| | | A.7 | Ús no previst | 5 | 75% | 6,975 | 34,875 | **Mitigar** | 10,4625 |
| | | A.11 | Accés no autoritzat | 7,5 | 100% | 9,3 | 69,75 | **Evitar** | 20,925 |
| **(L) Seu Central** | 9,3 | N.1 | Foc | 0,1 | 100% | 9,3 | 0,93 | Assumir | - |
| | | N.2 | Danys per aigua | 2,5 | 75% | 6,975 | 17,437 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 50% | 4,65 | 11,625 | Assumir | - |
| | | A.7 | Ús no previst | 5 | 75% | 6,975 | 34,875 | **Mitigar** | 10,4625 |
| | | A.11 | Accés no autoritzat | 7,5 | 100% | 9,3 | 69,75 | **Evitar** | 20,925 |
| **(L) Oficina Territorial** | 8,6 | N.1 | Foc | 0,1 | 100% | 8,3 | 0,83 | Assumir | - |
| | | N.2 | Danys per aigua | 2,5 | 75% | 5,975 | 14,93 | Assumir | - |
| | | N.9 | Origen meteorològic | 2,5 | 50% | 3,65 | 9,125 | Assumir | - |
| | | A.7 | Ús no previst | 5 | 75% | 6,45 | 32,25 | **Mitigar** | 9,675 |
| | | A.11 | Accés no autoritzat | 7,5 | 100% | 8,6 | 64,5 | **Evitar** | 19,35 |

Taula 30. Anàlisi de risc Instal·lacions (L)

| Actiu | Valor | Amenaça | | Prob | Degradació | Impacte | Risc inicial | Acció | Risc residual |
|---|---|---|---|---|---|---|---|---|---|
| **(P) Treballadors** | 6,4 | E.7 | Deficiències amb la organització | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | E.19 | Fuga de informació | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | E.28 | Indisponiblitat del personal | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | A.28 | Indisponiblitat del personal | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| | | A.29 | Extorsió | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| | | A.30 | Enginyeria social | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| **(P) Administradors** | 6,4 | E.7 | Deficiències amb la organització | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | E.19 | Fuga de informació | 5 | 25% | 1,6 | 24 | **Mitigar** | 7,2 |
| | | E.28 | Indisponiblitat del personal | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | A.28 | Indisponiblitat del personal | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| | | A.29 | Extorsió | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| | | A.30 | Enginyeria social | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| **(P) Proveïdors** | 6,4 | E.7 | Deficiències amb la organització | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | E.19 | Fuga de informació | 2,5 | 75% | 3,2 | 8 | Assumir | - |
| | | E.28 | Indisponiblitat del personal | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | A.28 | Indisponiblitat del personal | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| | | A.29 | Extorsió | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| | | A.30 | Enginyeria social | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| **(P) Clients** | 6,4 | E.7 | Deficiències amb la organització | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | E.19 | Fuga de informació | 5 | 25% | 1,6 | 8 | Assumir | - |
| | | E.28 | Indisponiblitat del personal | 5 | 75% | 4,8 | 24 | **Mitigar** | 7,2 |
| | | A.28 | Indisponiblitat del personal | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| | | A.29 | Extorsió | 2,5 | 75% | 4,8 | 12 | Assumir | - |
| | | A.30 | Enginyeria social | 2,5 | 75% | 4,8 | 12 | Assumir | - |

Taula 31. Anàlisi de risc Persones (P)

Els valors del risc no corresponen a la taula del punt 3.6 perquè aquesta és extreta de MAGERIT sense usar el càlcul de la pròpia fórmula (probabilitat x impacte). Per aquesta raó, la següent taula és l'emprada durant els nivells de risc de l'anàlisi feta. Com es pot veure, a partir de >50 és quan es considera de màxim nivell de risc (roig) mentre que <15 és verd (el valor de tall acceptable).

| RISC Probabilitat x Impacte | | PROBABILITAT | | | | |
|---|---|---|---|---|---|---|
| | | MB (0,1) | B (2,5) | M (5) | A (7,5) | MA (10) |
| IMPACTE | MA (10) | 1 | 25 | 50 | 75 | 100 |
| | A (7,5) | 0,75 | 18,75 | 37,5 | 56,25 | 75 |
| | M (5) | 0,5 | 12,5 | 25 | 37,5 | 50 |
| | B (2,5) | 0,25 | 6,25 | 12,5 | 18,75 | 25 |
| | MB (0,25) | 0,025 | 0,625 | 1,25 | 1,875 | 2,5 |

Taula 32. Fòrmula del càlcul del risc

Els punts a destacar de l'anàlisi de riscos de la cooperativa agrícola són els següents:

**Accions destacades:**

- S'ha aconseguit identificar tots els actius essencials per al funcionament de l'empresa, incloent-hi les dades sensibles, els sistemes informàtics i la infraestructura de xarxa.
- S'han estudiat les diverses amenaces potencials, que van des dels ciberatacs fins als errors humans i desastres naturals, per comprendre els perills als quals està exposada l'empresa i determinar el seu impacte.
- S'han proposat diverses mesures per abordar les amenaces identificades.
- S'ha identificat el risc inicial de cada actiu en cada situació amenaçant i també el residual després de l'aplicació del pla d'acció per assegurar que els riscos s'hagin reduït adequadament.

**Riscos identificats:**

- Els errors humans, com ara l'accés no autoritzat a les dades o la divulgació accidental de la informació confidencial, es reconeix com a risc rellevant.
- Les amenaces cibernètiques, com ara atacs de malware i intents d'intrusió també, especialment donada la importància de les dades sensibles que gestiona.

- La interrupció de les operacions a causa de desastres naturals, fallades del sistema o altres incidents podria tenir un impacte significatiu en la capacitat de l'empresa per funcionar de manera efectiva però és menys probable.

**Actius amb més risc:**

- Els actius amb més risc son la informació sensible, els serveis, els equips informàtics i les aplicacions informàtiques.
- Les amenaces que més es presenten per aquests actius són causades per errors dels usuaris i per accions malintencionades. Aquestes amenaces podrien manifestar-se de diverses maneres, com ara atacs de malware, phishing, accions no intencionades del personal, errors de configuració del sistema, etc.

**Estratègies per mitigar:**

- Les dades obtingudes sobre les accions tractades es mostren en la següent gràfica.

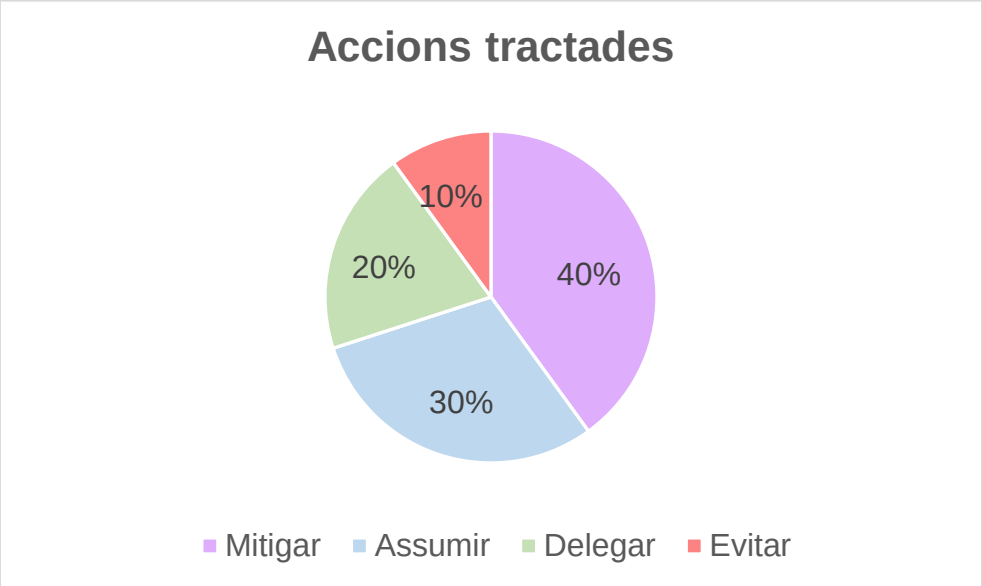


Figura 9. Proporcions de les accions tractades

Com es pot veure, la major part d'accions tractades són la mitigació (o millora) per a reduir el seu risc, seguit de la delegació en alguns casos i en rares ocasions s'evitarà, que són aquells on s'escull no participar en l'acció que podria fer que un fet amb risc es pugui produir. Com no es realista poder aplicar mesures a tots els riscs perquè no existeix pressupost il·limitat, a part que també hi ha bastantes amenaces que no tenen un risc elevat , aquestes són les que s'assumeixen.

## 4.4 Revisió i reflexió de la SoA

És important comprendre com es relaciona l'anàlisi de riscos i la SoA. La SoA és el document on es detallen les mesures o controls de seguretat que s'aplicaran al sistema d'informació de l'organització, d'acord amb la seva categorització. Aquesta categorització pot entendre's com "l'apetit de risc" de l'organització en relació amb els actius dins de l'abast del SGSI.

La categorització es realitza idealment en dos moments: un en funció del risc potencial (sense mesures o controls) i un altre en funció del risc resultant/residual (amb mesures o controls) que seran els riscos acceptables per a l'organització.

Per tant, s'ha de revisar el SoA, i tenir en compte com les mesures de seguretat que hi ha definides s'ajusten als riscos identificats durant l'anàlisi de riscos. Assegurant que les mesures o controls proposats siguin adequats per mitigar els riscos identificats i que estiguin alineats amb l'apetit de risc de l'organització.

**Revisió:**

Basant-nos en la Declaració d'Aplicabilitat presentada i l'anàlisi de riscos prèvia realitzat, es posa de manifest una tendència preocupant: la majoria de les amenaces i riscs identificats estan associats a errors humans i accions malintencionades.

Per sort, s'han tingut en compte els controls necessaris per afrontar els riscos que han sortit durant l'anàlisi de riscos realitzats, i s'assegura una coherència entre les amenaces i les accions implementades per mitigar-les. Els controls a destacar per a prioritzar la seva mitigació del risc serien entre altres, aquests:

Gestió de privilegis d'accés (8.2)

- Aquest control és crucial per mitigar els riscos associats a accions malintencionades, ja que restringeix l'accés a les dades només als usuaris autoritzats, gestionant eficaçment els privilegis d'accés mitjançant Microsoft 365 i altres eines.

Restricció d'accés a la informació (8.3)

- Donat que molts dels riscos identificats estan relacionats amb errors humans, és vital establir restriccions d'accés a la informació per garantir que només els usuaris autoritzats puguin accedir-hi. Tot i que aquest

control es troba en un estat repetible, cal millorar-lo per estandarditzar i centralitzar les restriccions d'accés.

Gestió de la configuració (8.9)

- Aquest control és fonamental per assegurar que tots els equips estiguin configurats de manera segura i que s'implementin els controls necessaris per protegir-los contra amenaces conegudes. Malgrat estar definit, es reconeix la necessitat de millora, especialment en la configuració de seguretat.

Prevenció de fuites de dades (8.12)

- A causa de la sensibilitat de les dades de l'organització, és essencial implementar controls per prevenir la fuga d'informació. Encara que aquest control es troba en un estat repetible, es reconeix que requereix una major dedicació per garantir una protecció eficaç.

Per tant, en la declaració d'aplicabilitat la majoria dels controls han estat identificats i implementats, tot i que molts d'ells en un estat "mitjà" o "baix", però amb consciència de pujar la seva implicació en resposta als riscos detectats.

Per exemple, es tenen en compte aspectes que fluixegen més com la manca de filtratge web, ja que els errors humans poden ser explotats a través de l'accés a contingut maliciós o no autoritzat a la xarxa. Això, juntament amb altres mancances de seguretat, com la falta de protecció antimalware, pot augmentar significativament l'exposició a amenaces externes i és un aspecte prioritari.

A més, en àrees com la seguretat en el cicle de vida dels desenvolupaments i la codificació segura, la manca de protocols específics pot augmentar el risc d'atacs malintencionats o errors involuntaris que podrien comprometre la seguretat dels sistemes.

En resum, la revisió de la Declaració d'Aplicabilitat i l'Anàlisi de Riscos destaca la necessitat crítica de prioritzar els controls i les mesures de seguretat destinades a mitigar els riscos derivats d'errors humans i accions malintencionades. Aquesta àrea necessita una atenció especial per garantir la protecció efectiva dels actius de la companyia i la prevenció d'incidents de seguretat greus.

# 5. Propostes de Projectes

Un cop realitzat l'Anàlisi de Riscos i per tant coneixent el nivell de risc actual a la cooperativa, el Comitè de Seguretat planteja una sèrie de projectes per a millorar l'estat de la seguretat amb l'objectiu de reduir el risc perquè sigui igual o inferior a l'acceptable.

Aquestes propostes ajudarien a mitigar el risc actual de la cooperativa gràcies al compliment ISO en base a les recomanacions associades a les amenaces identificades. S'incidirà, no només en la millora de la gestió de la seguretat, sinó també en possibles beneficis col·laterals com poden ser: l'optimització de recursos, la millora de la gestió de processos i tecnologies presents a l'organització analitzada.

Cada proposta de projecte inclou aquest esquema general com a estructura:

- Nom del projecte i codi.
- Pressupost que suposa i planificació del termini segons l'escala Curt, Mitjà i Llarg.
- Objectiu de millora que complirà el projecte en la seva implantació.
- Controls identificats de la normativa ISO 27002.
- Actius que poden ser afectats positivament en la implementació del projecte.
- Amenaces a tractar amb la implementació del projecte detectada a l'anàlisi de risc.
- Prioritat del projecte amb una escala de Baixa, Mitjana i Alta.
- Responsable i membres implicats en la realització del projecte.
- Punts de control o mesuradors que permeten verificar el resultat i comprovar l'execució del projecte.

Els costos dels projectes es definiran a través d'una estimació de costos, que implica, segons el context de l'empresa (veure en el punt 2) la identificació, l'anàlisi i la quantificació de tots els elements que contribueixen als costos del projecte. Especialment, per a definir els costos de cada projecte es tindrà en compte que el nombre de membres de la cooperativa és de 60, i segons el tipus, es podria estimar la mà d'obra i els especialistes per al seu desenvolupament.

## 5.1 Propostes d'àmbit organitzatiu

<table>
<tr><td>Codi: PROJ - 1</td><td colspan="2">Nom: Programa de formació i conscienciació en seguretat de la informació</td></tr>
<tr><td>Pressupost: 35.000 €</td><td>Planificació: Llarg Termini</td><td>Prioritat: Alta</td></tr>
<tr><td colspan="3">Objectiu: Implementar un programa de formació i conscienciació sobre seguretat de la informació per als membres de la cooperativa amb l'objectiu de millorar la comprensió i el compliment de les polítiques i procediments de seguretat.</td></tr>
<tr><td colspan="3">Descripció: A causa del gra nombre d'amenaces detectades en errors humans, aquest projecte té com a objectiu principal desenvolupar i implementar un programa de formació integral sobre seguretat de la informació per a tots els membres de l'organització. Aquest programa inclourà sessions de formació presencials, material educatiu, campanyes de conscienciació i proves pràctiques per garantir l'aprenentatge en tot l'equip.</td></tr>
<tr><td colspan="3">Controls ISO 27002:<br>Control 5.1 Polítiques de seguretat de la informació<br>Control 6.3. Conscienciació, educació i formació en seguretat de la informació<br>Control 6.7. Teletreball<br>Control 7.2. Controles físics de entrada<br>Control 8.3. Restricció del accés a la informació<br>Control 8.16. Seguiment de activitats<br>Control 8.20. Seguretat de xarxes<br>Control 8.25. Seguretat en el cicle de vida del desenvolupament</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>E.1 Errors d'usuaris<br>E.2 Errors d'administrador<br>E.8 Difusió de software maligne<br>E.15 Alteració accidental de la informació<br>E.18 Destrucció de la informació<br>E.19 Fuga de informació<br>A.6 Abús de privilegis d'accés<br>A.7 Ús no previst<br>A.8 Difusió de software maligne<br>A.11 Accés no autoritzat</td><td>Actius afectats:<br>Dades dels membres<br>Dades dels clients<br>Dades financeres<br>Registres de nòmines<br>Servidors<br>Hardware (Tot)<br>Aplicacions informàtiques (Totes)<br>Suports d'informació<br>Totes les persones de la cooperativa.</td></tr>
<tr><td colspan="2">Responsable: CIO</td><td>Membres implicats: CISO, DPD, CTO, Responsables dels departaments.</td></tr>
</table>

Taula 33. Proposta de Projecte 1

Per assegurar que sigui un procés de millora continua, es realitzaran reunions periòdiques de seguiment de la implementació del programa de formació i conscienciació en seguretat de la informació a més de monitorització. A més, el CISO estarà assabentat de les revisions regulars de les sessions per avaluar-ne l'eficàcia i fer-ne ajustaments si és necessari. El pressupost abasta els recursos educatius, les sessions de formació presencials, les campanyes de conscienciació i els costos de personal.

<table>
<tr><td>Codi: PROJ - 2</td><td colspan="2">Nom: Programa de formació en l'ús segur de les aplicacions de la cooperativa</td></tr>
<tr><td>Pressupost: 25.000 €</td><td>Planificació: Llarg Termini</td><td>Prioritat: Alta</td></tr>
<tr><td colspan="3">Objectiu: Durant l'anàlisi de riscs s'ha detectat problemàtiques en l'ús de les aplicacions i eines informàtiques de la cooperativa. Per aquesta raó, l'objectiu d'aquest projecte és desenvolupar i implementar un programa de formació destinat als membres de la cooperativa per assegurar un ús segur i eficient de les aplicacions utilitzades a l'organització.</td></tr>
<tr><td colspan="3">Descripció: Proporcionar formació integral sobre l'ús segur i adequat de les diverses aplicacions utilitzades a la cooperativa. El programa de formació constarà de manuals d'ús, sessions pràctiques amb les guies d'ús i bones pràctiques, i proves pràctiques per garantir que tots els membres de l'organització estiguin adequadament informats i formats sobre l'ús correcte de les aplicacions.</td></tr>
<tr><td colspan="3">Controls ISO 27002:<br>Control 6.3. Conscienciació, educació i formació en seguretat de la informació<br>Control 7.1: Gestió d'actius<br>Control 8.6: Gestió dels canvis<br>Control 8.7: Distribució d'informació<br>Control 8.8: Gestió de l'accés de l'usuari<br>Control 8.10: Monitorització de l'ús del sistema d'informació<br>Control 8.11: Protecció de la informació del sistema</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>E.1 Errors d'usuaris<br>E.2 Errors d'administrador<br>E.7: Deficiències amb la organització<br>E.10: Errors de seqüència<br>E.15: Alteració accidental de la informació<br>A.7: Ús no previst<br>A.8: Difusió de software maligne<br>A.22: Manipulació de programes</td><td>Actius afectats:<br>Aplicacions informàtiques (SW)<br>Dades manipulades a través del SW<br>Dispositius on s'executen (HW)<br>Treballadors que utilitzen el software</td></tr>
<tr><td colspan="2">Responsable: CIO</td><td>Membres implicats: CISO, DPD, CTO, Responsables dels departaments.</td></tr>
</table>

Taula 34. Proposta de Projecte 2

Per assegurar que el programa de formació sigui un procés de millora continua, es realitzaran revisions periòdiques de les sessions de formació i es recolliran feedbacks dels participants (mitjançant formularis Google Forms) per avaluar-ne l'eficàcia i fer-ne ajustaments si és necessari. A més, es realitzarà un seguiment de l'ús de les aplicacions per garantir el compliment de les polítiques i procediments establerts.

El pressupost inclourà els recursos necessaris per al desenvolupament i la implementació del programa de formació, així com els costos de personal i materials educatius.

<table>
<tr><th>Codi: PROJ - 3</th><th colspan="2">Nom: Programa de seguretat en l'ús de dispositius mòbils i portàtils</th></tr>
<tr><td>Pressupost: 10.000 €</td><td>Planificació: Mig Termini</td><td>Prioritat: Mitja</td></tr>
<tr><td colspan="3">Objectiu: Implementar un programa integral de seguretat per a l'ús de dispositius mòbils i portàtils a la cooperativa, amb l'objectiu de garantir la protecció de la informació sensible i reduir els riscos de seguretat associats a aquests dispositius.</td></tr>
<tr><td colspan="3">Descripció: Fins el moment, no es fa firmar als treballadors quan reben un d'aquests dispositius. Per tant, aquest projecte té com a objectiu principal desenvolupar i implementar un programa de seguretat que abordi els riscos associats amb l'ús de dispositius mòbils i portàtils a la cooperativa.</td></tr>
<tr><td colspan="3">Controls ISO 27002:<br>Control 6.3. Conscienciació, educació i formació en seguretat de la informació<br>Control 8.8. Gestió de l'equipament dels usuaris<br>Control 8.10. Seguretat de l'equipament fora de les instal·lacions<br>Control 8.12. Polítiques de treball remot<br>Control 9.3. Gestió dels dispositius mòbils<br>Control 9.4. Ús adequat de les aplicacions mòbils<br>Control 10.1. Gestió de les comunicacions i operacions</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>E.1 Errors d'usuaris<br>E.2 Errors d'administrador<br>E.8 Difusió de software maligne<br>E.15 Alteració accidental de la informació<br>E.18 Destrucció de la informació<br>E.19 Fuga de informació<br>E.25 Pèrdua d'equips<br>A.6 Abús de privilegis d'accés<br>A.7 Ús no previst<br>A.8 Difusió de software maligne<br>A.11 Accés no autoritzat</td><td>Actius afectats:<br>Dispositius mòbils (HW)<br>Portàtils (HW)</td></tr>
<tr><td colspan="2">Responsable: CTO</td><td>Membres implicats: CISO, CIO, DPD, Responsables dels departaments.</td></tr>
</table>

Taula 35. Proposta de Projecte 3

Per garantir que el programa de seguretat en l'ús de dispositius mòbils i portàtils segueixi un procés de millora contínua, s'implementaran avaluacions regulars de la normativa afegida a la política de seguretat i un monitoratge dels dispositius per al seu correcte seguiment d'aquests (amb etiquetatge oportú).

<table>
<tr><th>Codi: PROJ - 4</th><th colspan="2">Nom: Política d’acords de confidencialitat dels treballadors i proveïdors</th></tr>
<tr><td colspan="2">Pressupost: 4.500 €</td><td>Planificació: Curt Termini</td><td>Prioritat: Alta</td></tr>
<tr><td colspan="4">Objectiu: Establir i implementar en la Política de Seguretat acords de confidencialitat per a treballadors i proveïdors per protegir la informació sensible de la cooperativa i evitar filtracions de dades.</td></tr>
<tr><td colspan="4">Descripció: Aquest projecte té com a objectiu principal establir i implementar acords de confidencialitat per als treballadors i proveïdors de la cooperativa. Aquests acords definiran clarament les responsabilitats i les obligacions relacionades amb la protecció de la informació sensible i la prevenció de filtracions de dades. Això inclourà l'avaluació de les polítiques i els procediments existents, la redacció dels acords de confidencialitat, la formació del personal sobre les seves responsabilitats i la supervisió del compliment dels acords.</td></tr>
<tr><td colspan="4">Controls ISO 27002:<br>Control 5.1 Polítiques de seguretat de la informació<br>Control 6.6 Acords de confidencialitat o no divulgació</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>E.19 Fuga de informació<br>E.20 Interrupció de la disponibilitat del sistema<br>E.21 Pèrdua de funcionalitat de la informació<br>E.22 Interrupció de la integritat de la informació</td><td colspan="2">Actius afectats:<br>Informació dels membres (D)<br>Dades dels clients (D)<br>Informació financera (D)<br>Registres nòmines (D)<br>Treballadors (P)<br>Proveïdors (P)</td></tr>
<tr><td colspan="2">Responsable: DPD</td><td colspan="2">Membres implicats: CISO, Responsable RRHH, Cap departament gestió i administració i de negoci i mercat.</td></tr>
</table>

Taula 36. Proposta de Projecte 4

Aquest projecte s'executarà en diverses fases, incloent l'avaluació de les necessitats d'acords de confidencialitat, la redacció i revisió dels acords, la formació del personal sobre les seves obligacions, la implementació de mecanismes de supervisió i el seguiment del compliment dels acords per part del personal i els proveïdors.

## 5.2 Propostes d'àmbit tecnològic

<table>
<tr><td>Codi: PROJ - 5</td><td colspan="2">Nom: Instal·lació d'una consola centralitzada antimalware</td></tr>
<tr><td>Pressupost: 12.000 €</td><td>Planificació: Mig Termini</td><td>Prioritat: Alta</td></tr>
<tr><td colspan="3">Objectiu: Tenir major control de l'estat de l'antivirus de tots el equips de la cooperativa a través de la implementació d'una consola centralitzada antimalware per gestionar de manera eficient la seguretat dels equips.</td></tr>
<tr><td colspan="3">Descripció: Aquest projecte té com a objectiu principal implementar una consola centralitzada antimalware per gestionar la seguretat dels equips informàtics a la cooperativa agrícola. La consola proporcionarà una plataforma central des d'on s'administrarà la configuració, la supervisió i la resposta a les amenaces de malware en tots els equips de l'organització. Es realitzarà una integració amb els sistemes existents i es configurarà la consola perquè proporcioni informació en temps real sobre l'estat de la seguretat, incloent alertes i informes detallats.</td></tr>
<tr><td colspan="3">Controls ISO 27002:<br>Control 8.3. Restricció d'accés a la informació<br>Control 8.7. Controls contra el codi maliciós<br>Control 8.8. Gestió de vulnerabilitats tècniques<br>Control 8.13. Còpies de seguretat de la informació<br>Control 8.24. Ús de la criptografia</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>E.8 Difusió de software maligne<br>E.18 Destrucció de la informació<br>A.8 Difusió de software maligne<br>A.24 Denegació de servei</td><td>Actius afectats:<br>Antivirus (SW)<br>Informació dels membres (D)<br>Dades dels clients (D)<br>Informació financera (D)<br>Registres nòmines (D)</td></tr>
<tr><td colspan="2">Responsable: CTO</td><td>Membres implicats: CISO, CIO, DPD, Equip T.I</td></tr>
</table>

Taula 37. Proposta de Projecte 5

Tot i ja disposar d'un antivirus, la cooperativa ha rebut durant l'anàlisi de riscos grans valors de risc en els actius de serveis i software. Per aquesta raó, es decideix portar una petita inversió en actualitzar-lo per millorar la seva robustesa i eficàcia amb una consola centralitzada que controli l'estat del antivirus en cada equip.

Aquest programa d'actualització s'executarà de manera iterativa per assegurar que sigui un procés de millora continua, amb revisions periòdiques per avaluar l'eficàcia de les mesures implementades i fer-ne ajustaments si cal.

<table>
<tr><th>Codi: PROJ - 6</th><th colspan="2">Nom: Programa de millora del sistema de còpies de seguretat</th></tr>
<tr><td>Pressupost: 8.000 €</td><td>Planificació: Curt Termini</td><td>Prioritat: Mitja</td></tr>
<tr><td colspan="3">Objectiu: Millorar el sistema de còpies de seguretat de la cooperativa per garantir la disponibilitat i la integritat de les dades en cas de desastre o pèrdua de dades.</td></tr>
<tr><td colspan="3">Descripció: Aquest projecte té com a objectiu principal millorar el sistema de còpies de seguretat actual de la cooperativa per aconseguir una gestió més eficient i fiable de les còpies de seguretat. Això inclourà l'avaluació de les necessitats de còpies de seguretat de cada sistema i aplicació, la implementació de procediments estandarditzats de còpies de seguretat i la millora de les pràctiques de restauració de dades.</td></tr>
<tr><td colspan="3">Controls ISO 27002:<br>Control 8.13. Còpies de seguretat de la informació<br>Control 8.14. Redundància de les instal·lacions de processament d'informació<br>Control 8.33. Dades de prova</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>E.18 Destrucció de la informació<br>E.19 Fuga de informació<br>E.20 Interrupció de la disponibilitat del sistema<br>E.21 Pèrdua de funcionalitat de la informació</td><td>Actius afectats:<br>Informació dels membres (D)<br>Dades dels clients (D)<br>Informació financera (D)<br>Registres nòmines (D)<br>Aplicacions informàtiques (Totes)<br>Serveis.</td></tr>
<tr><td colspan="2">Responsable: CTO</td><td>Membres implicats: CISO, CIO, Equip T.I.</td></tr>
</table>

Taula 38. Proposta de Projecte 6

L'equip T.I té la responsabilitat de realitzar backups, però aquesta implementació no està ben definida ni hi ha una política clara. Cal actualitzar-ho i adaptar-ho al volum de dades que correspon en la cooperativa. De la mateixa manera, podria ser necessària realitzar una migració de dades al núvol del Office 365. Per tant, tot i no ser un procediment prioritari, s'ha de millorar per passar a un major nivell de maduresa i reduir a la vegada el risc.

<table>
<tr><th>Codi: PROJ - 7</th><th colspan="2">Nom: Pla de desenvolupament de codi segur</th></tr>
<tr><td>Pressupost: 17.000 €</td><td>Planificació: Mig Termini</td><td>Prioritat: Mitja</td></tr>
<tr><td colspan="3">Objectiu: Establir i implementar un pla de desenvolupament de codi segur per millorar la seguretat dels sistemes i aplicacions de la cooperativa i reduir els riscos relacionats amb vulnerabilitats de codi.</td></tr>
<tr><td colspan="3">Descripció: Aquest projecte té com a objectiu principal definir i implementar un pla de desenvolupament de codi segur per a tots els projectes de desenvolupament de software de la cooperativa. Aquest pla inclourà l'adopció de les millors pràctiques en matèria de seguretat del codi, la realització d'anàlisis de vulnerabilitats i la implementació de mesures de protecció en tot el cicle de vida del desenvolupament de software. A més, s'oferirà formació als desenvolupadors sobre les tècniques i les eines per escriure codi segur i es realitzarà un seguiment del compliment del pla.</td></tr>
<tr><td colspan="3">Controls ISO 27002:<br>Control 8.26 Requisits de seguretat de les aplicacions<br>Control 8.27 Arquitectura segura de sistemes i principis d'enginyeria<br>Control 8.28 Codificació segura<br>Control 8.29 Proves de seguretat en desenvolupament i acceptació<br>Control 8.30 Externalització del desenvolupament de programari<br>Control 8.31 Separació dels recursos de desenvolupament, prova i operació<br>Control 8.32 Gestió de canvis</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>E.8 Difusió de software maligne<br>E.18 Destrucció de la informació<br>E.19 Fuga de informació<br>E.20 Interrupció de la disponibilitat del sistema<br>E.21 Pèrdua de funcionalitat de la informació<br>E.22 Interrupció de la integritat de la informació</td><td>Actius afectats:<br>Informació dels membres (D)<br>Dades dels clients (D)<br>Informació financera (D)<br>Registres nòmines (D)<br>Aplicacions informàtiques (Totes)</td></tr>
<tr><td colspan="2">Responsable: CTO</td><td>Membres implicats: CISO, Equip T.I</td></tr>
</table>

Taula 39. Proposta de Projecte 7

Aquest projecte es desenvoluparà en diverses etapes que calen estar degudament documentades: l'anàlisi de les pràctiques de desenvolupament de codi actuals, la definició i implementació de les noves polítiques i procediments de seguretat del codi, i el seguiment i la revisió regulars del compliment del pla de desenvolupament de codi segur.

<table>
<tr><th colspan="2">Codi: PROJ - 8</th><th colspan="2">Nom: Implementació de protecció criptogràfica de les dades</th></tr>
<tr><td colspan="2">Pressupost: 42.000 €</td><td>Planificació: Llarg Termini</td><td>Prioritat: Mitja</td></tr>
<tr><td colspan="4">Objectiu: Implementar un sistema de protecció criptogràfica de les dades per garantir la confidencialitat i la integritat de la informació sensible emmagatzemada i transmesa per la cooperativa agrícola. Aquesta implementació millorarà la seguretat dels sistemes informàtics i minimitzarà el risc d'accés no autoritzat a les dades.</td></tr>
<tr><td colspan="4">Descripció: Aquest projecte té com a objectiu principal implementar una solució criptogràfica robusta per protegir les dades sensibles emmagatzemades i transmeses pels sistemes informàtics de la cooperativa agrícola. Es realitzarà una avaluació exhaustiva de les necessitats de seguretat de la informació i s'identificaran les àrees crítiques on es requereix protecció criptogràfica. Es seleccionaran les tecnologies criptogràfiques més adequades i s'establiran polítiques i procediments per a la gestió de claus, l'encriptació de dades i altres aspectes rellevants de la protecció criptogràfica.</td></tr>
<tr><td colspan="4">Controls ISO 27002:<br>Control 8.23. Filtrat de webs<br>Control 8.24. Ús de la criptografia<br>Control 8.26. Requisits de seguretat de les aplicacions</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>E.19 Fuga de informació<br>A.5 Suplantació d’identitat<br>A.11 Accés no autoritzat<br>A.22 Manipulació dels equips<br>A.25 Robatori</td><td colspan="2">Actius afectats:<br>Dades dels clients (D)<br>Informació financera (D)<br>Informació de la producció agrícola (D)<br>Informació de proveïdors (D)<br>Aplicacions informàtiques (Totes)<br>Servidors (Tots)</td></tr>
<tr><td colspan="2">Responsable: CTO</td><td colspan="2">Membres implicats: CISO, CIO, Auditor Intern, DPD, Responsable T.I.</td></tr>
</table>

Taula 40. Proposta de Projecte 8

Per assegurar la millora contínua, la cooperativa agrícola inclourà en el model d’avaluacions i reunions regulars aquest contingut en l’àrea T.I per avaluar l'eficàcia del sistema. De la mateixa manera, en cas que sigui necessari, es buscarà el reclutament de personal addicional amb la formació pertinent en protecció criptogràfica, monitoratge i informes d'incidents.

Aquest enfocament garantirà que la protecció criptogràfica de les dades sigui sempre actualitzada i eficaç, mantenint-se alineada amb les necessitats de seguretat en evolució de la cooperativa.

<table>
<tr><th>Codi: PROJ - 9</th><th colspan="2">Nom: Pla de continuïtat del negoci</th></tr>
<tr><td>Pressupost: 7.000 €</td><td>Planificació: Mig Termini</td><td>Prioritat: Alta</td></tr>
<tr><td colspan="3">Objectiu: Desenvolupar i implementar un Pla de Continuïtat del Negoci per assegurar la resiliència de la cooperativa davant de possibles interrupcions o incidents que puguin afectar les seves operacions. Aquest pla garantirà la disponibilitat dels serveis essencials i la protecció dels actius crítics de la cooperativa.</td></tr>
<tr><td colspan="3">Descripció: Aquest projecte té com a objectiu principal desenvolupar i implementar un pla de continuïtat del negoci exhaustiu i eficaç que asseguri la resiliència de les operacions de la cooperativa davant de diversos tipus d'incidents, com ara desastres naturals, fallades de tecnologia, interrupcions del servei, entre altres. Es realitzarà una avaluació completa dels riscos que podrien afectar la continuïtat del negoci i s'identificaran les necessitats específiques de continuïtat en funció dels processos de negoci crítics. S’inclourà estratègies i mesures per respondre a diferents escenaris d'emergència, procediments d'alerta i de resposta, protocols de comunicació interna i externa, entre altres aspectes rellevants.</td></tr>
<tr><td colspan="3">Controls ISO 27002:<br>Control 5.24. Planificació i Preparació de la Gestió d'Incidents de Seguretat de la Informació<br>Control 5.25. Avaluació i Decisió sobre els Esdeveniments de Seguretat de la Informació<br>Control 5.26. Resposta a Incidents de Seguretat de la Informació<br>Control 5.27. Aprenentatge dels Incidents de Seguretat de la Informació<br>Control 5.29. Seguretat de la Informació Durant la Interrupció<br>Control 5.30. Preparació per a les TIC per a la Continuïtat del Negoci<br>Control 5.31. Identificació de Requisits Legals, Reglamentaris i Contractuals</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>[N] Desastres Natural – Tots<br>[I] Origen Industrial - Tots<br>E.8 Difusió de software maligne<br>E.18 Destrucció de la informació<br>E.20 Interrupció de la disponibilitat del sistema<br>E.21 Pèrdua de funcionalitat de la informació<br>A.15 Modificació deliberada de la informació<br>A.18 Destrucció de la informació<br>A.24 Denegació de Servei<br>A.25 Robatori<br>A.26 Atac Destructiu</td><td>Actius afectats:<br>Informació dels membres (D)<br>Dades dels clients (D)<br>Informació financera (D)<br>Registres nòmines (D)<br>Aplicacions informàtiques (Totes)<br>Hardware (Tot)<br>Serveis (Tots)<br>Equipament auxiliar (Tot)<br>Xarxes de comunicació (Totes)<br>Instal·lacions (Totes)</td></tr>
<tr><td colspan="2">Responsable: CISO</td><td>Membres implicats: CEO, CIO, CTO, Auditor Intern, DDP, Responsable RRHH.</td></tr>
</table>

Taula 41. Proposta de Projecte 9

Perquè sigui un procés de millora continua es realitzaran auditories periòdiques (mínim una cada any) per avaluar l'eficàcia del pla, identificar possibles desviacions respecte als objectius establerts i recomanar accions correctives.

<table>
<tr><td>Codi: PROJ - 10</td><td colspan="2">Nom: Implementació d’un sistema de gestió d’informació i esdeveniments de seguretat</td></tr>
<tr><td>Pressupost: 25.000 €</td><td>Planificació: Llarg Termini</td><td>Prioritat: Alta</td></tr>
<tr><td colspan="3">Objectiu: Implementar un SIEM per monitorar, analitzar i respondre proactivament a les amenaces de seguretat informàtica a la cooperativa agrícola.</td></tr>
<tr><td colspan="3">Descripció: Aquest projecte té com a objectiu principal implementar un SIEM integrat amb les infraestructures existents de la cooperativa agrícola. Es realitzarà una avaluació dels requisits de monitoratge i gestió de la seguretat de la informació, identificant les fonts de dades rellevants, els protocols de comunicació i els processos de gestió d'incidents.<br><br>El SIEM seleccionat es configurarà per recopilar, normalitzar i correlacionar els esdeveniments de seguretat procedents de múltiples fonts, com ara registres de sistemes, dispositius de xarxa, aplicacions i servidors.<br><br>A més, es definiran procediments i protocols de resposta a incidents per abordar ràpidament les amenaces detectades i mitigar els seus impactes. Es realitzaran simulacions d'atacs i exercicis de resposta a incidents per preparar el personal i avaluar l'eficàcia del SIEM en la detecció i resposta a amenaces.</td></tr>
<tr><td colspan="3">Controls ISO 27002:<br>Control 8.15. Registres<br>Control 8.16 Seguiment d'activitats</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>A.3. Accés no autoritzat<br>A.5 Suplantació d’identitat<br>A.10. Dany accidental<br>A.11 Accés no autoritzat<br>A.13. Disseminació de programari maliciós<br>A.22 Manipulació dels equips<br>A.25 Robatori<br>A.28. Errors dels empleats</td><td>Actius afectats:<br>Dades dels clients (D)<br>Informació financera (D)<br>Informació de la producció agrícola (D)<br>Informació de proveïdors (D)<br>Aplicacions informàtiques (Totes)<br>Servidors (Tots)</td></tr>
<tr><td colspan="2">Responsable: CIO</td><td>Membres implicats: CISO i CTO</td></tr>
</table>

Taula 42. Proposta de Projecte 10

Per assegurar la millora contínua, la cooperativa agrícola inclourà en el model d’avaluacions i reunions regulars aquest contingut en l’àrea de seguretat de la informació per avaluar l'eficàcia del SIEM. De la mateixa manera, es realitzarà formació específica al personal relativa a la gestió i monitoratge del SIEM per garantir que sigui utilitzat de manera efectiva i eficient. Aquest enfocament garantirà que el SIEM sigui sempre actualitzat i eficaç, mantenint-se alineat amb les necessitats de seguretat en evolució de la cooperativa.

## 5.3 Altres propostes

<table>
<tr><th colspan="2">Codi: PROJ - 11</th><th colspan="2">Nom: Programa de millora de la seguretat física en les instal·lacions</th></tr>
<tr><td colspan="2">Pressupost: 10.000 €</td><td colspan="2">Planificació: Mig Termini</td><td>Prioritat: Mitja</td></tr>
<tr><td colspan="5">Objectiu: Implementar mesures per millorar la seguretat física de les instal·lacions de la cooperativa amb l'objectiu de protegir els actius i garantir la integritat i la confidencialitat de la informació.</td></tr>
<tr><td colspan="5">Descripció: Aquest projecte té com a objectiu principal identificar les àrees de millora de la seguretat física de les instal·lacions de la cooperativa i implementar les mesures adequades per abordar-les. Això pot incloure la instal·lació de sistemes de control d'accés, la millora de la vigilància de la seguretat, l'optimització dels sistemes d'alarma i altres mesures preventives.</td></tr>
<tr><td colspan="5">Controls ISO 27002:<br>Control 7.1. Perímetre de seguretat física<br>Control 7.2. Controls físics d’entrada<br>Control 7.3. Seguretat d'oficines, despatxos i recursos<br>Control 7.4. Vigilància de la seguretat física<br>Control 7.5. Protecció contra les amenaces externes i ambientals<br>Control 7.6. El treball en àrees segures<br>Control 7.7. Política de lloc de treball clar i pantalla neta<br>Control 7.8. Emplaçament i protecció d'equips</td></tr>
<tr><td colspan="2">Amenaces tractades:<br>E.8 Difusió de software maligne<br>A.7 Ús no previst<br>A.11 Accés no autoritzat<br>A.25 Robatori</td><td colspan="3">Actius afectats:<br>Planta de processament (L)<br>Seu central (L)<br>Oficina territorial (L)<br>Equips de climatització (AUX)<br>Càmeres de seguretat (AUX)</td></tr>
<tr><td colspan="2">Responsable: CISO</td><td colspan="3">Membres implicats: Responsable de RRHH i Empresa subcontractada física.</td></tr>
</table>

Taula 43. Proposta de Projecte 11

És cert que el control d’accés i la seguretat física de la cooperativa està al càrrec d’una empresa subcontractada, per aquesta raó, es col·laborarà amb ells per evitar que hi hagi cap incident, perquè tot i que no s’hi ha detectat mai, hi ha possibles deficiències detectades durant l’anàlisi de risc i aquest ha de disminuir lleugerament.

De nou, per assegurar que sigui un procés de millora continua, s'organitzaran reunions periòdiques per avaluar l'eficàcia de les mesures implementades i fer-ne ajustaments si cal.

| Codi: PROJ - 12 | Nom: Programa de millora de la gestió de RRHH | |
|---|---|---|
| **Pressupost:** 6.000 € | **Planificació:** Mig Termini | **Prioritat:** Baixa |
| **Objectiu:** Optimitzar la gestió dels recursos humans a la cooperativa agrícola mitjançant la implementació de processos més eficients i l'ús de tecnologies adequades. Aquesta millora permetrà una gestió més efectiva del personal i contribuirà al desenvolupament i benestar dels empleats. | | |
| **Descripció:** Aquest projecte té com a objectiu millorar la gestió dels recursos humans a la cooperativa agrícola mitjançant la implementació de processos més eficients i l'ús de tecnologies adequades. Es realitzarà una revisió exhaustiva dels processos actuals de gestió del personal per identificar àrees d'optimització i es proposaran millores concretes. Es buscarà implementar un sistema de gestió dels recursos humans basat en tecnologia que faciliti tasques com la gestió de nòmines, seguiment de l'assistència, avaluació del rendiment i gestió dels permisos. A més, es proporcionarà formació al personal per garantir una transició suau cap a les noves tecnologies i processos. | | |
| **Controls ISO 27002:**<br>Control 6.1. Comprovació<br>Control 6.3. Conscienciació, educació i formació en seguretat de la informació | | |
| **Amenaces tractades:**<br>E.28 Indisponiblitat del personal<br>A.29 Extorsió<br>A.30 Enginyeria social | **Actius afectats:**<br>Treballadors (P)<br>Administradors (P) | |
| **Responsable:** Responsable de RRHH | **Membres implicats:** CEO i CISO | |

Taula 44. Proposta de Projecte 12

El procediment de contractació i de gestió dels processos d'identificació de personal ha de rebre una actualització que permeti buscar, per exemple, antecedents.

Per assegurar la seva millora continua, s'establiran indicadors clau de rendiment (KPIs) per avaluar l'eficàcia del nou sistema de gestió dels recursos humans, com ara el temps d'ocupació de les posicions, la taxa de rotació del personal i la satisfacció dels empleats.

## 5.4 Pla d’execució i resultats

Els projectes no són seqüencials entre ells, el que significa que un pot començar i acabar en les dates especificades independentment dels altres projectes, ja que aquests no depenen d’altres mentre s’executen.

Les dates s'han determinat tenint en compte la naturalesa dels projectes i les seves prioritats, permetent algunes superposicions i assegurant que els projectes comencin en moments més adequats segons les seves necessitats i dependències.

Els projectes es divideixen en propostes organitzatives, tècniques i altres propostes per reflectir les diferents àrees d'enfocament. Les propostes organitzatives, com ara el programa de formació i conscienciació en seguretat de la informació (PROJ-1) i el programa de formació en l'ús segur de les aplicacions (PROJ-2) tenen dates d'inici coincidents perquè poden ser executades en paral·lel sense afectar-se l'un a l'altre.

Altres propostes, com el programa de millora de la seguretat física en les instal·lacions (PROJ-10), es poden planificar per a un moment posterior, com a l'estiu, quan les condicions són més favorables per a aquest tipus d'activitats.

Cadascun dels projectes té la seva pròpia prioritat, des de propostes organitzatives fins a altres propostes, i això es té en compte a l'hora de planificar les seves dates d'inici i finalització. Per exemple, el pla de continuïtat del negoci (PROJ-9), considerat una prioritat alta, té una data d'inici posterior per garantir que tots els recursos necessaris estiguin disponibles.

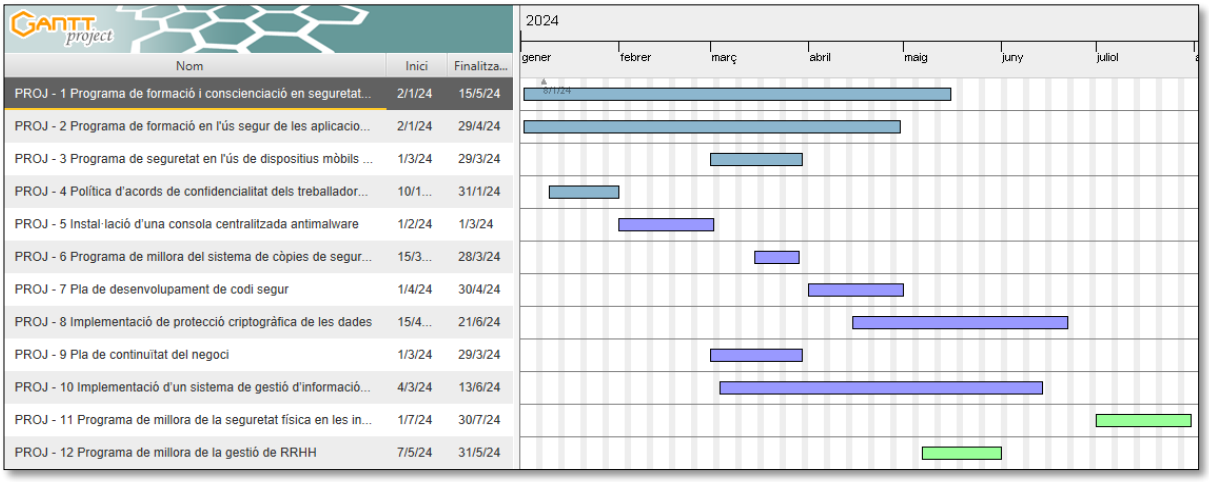


Figura 10. Proporcions de les accions tractades

| Codi | Projecte | Inici | Fi | Cost | Ordre de prioritat |
|---|---|---|---|---|---|
| **Propostes organitzatives** | | | | | |
| **PROJ – 1** | Programa de formació i conscienciació en seguretat de la informació | 02/01/2024 | 15/05/2024 | 35.000 € | 1 |
| **PROJ – 2** | Programa de formació en l'ús segur de les aplicacions de la cooperativa | 02/01/2024 | 29/04/2024 | 25.000 € | 2 |
| **PROJ – 3** | Programa de seguretat en l'ús de dispositius mòbils i portàtils | 01/03/2024 | 29/03/2024 | 10.000 € | 5 |
| **PROJ – 4** | Política d'acords de confidencialitat dels treballadors i proveïdors | 10/01/2024 | 31/01/2024 | 4.500 € | 3 |
| **Propostes tècniques** | | | | | |
| **PROJ – 5** | Instal·lació d'una consola centralitzada antimalware | 01/02/2024 | 02/03/2024 | 12.000 € | 4 |
| **PROJ – 6** | Programa de millora del sistema de còpies de seguretat | 15/03/2024 | 28/03/2024 | 8.000 € | 8 |
| **PROJ – 7** | Pla de desenvolupament de codi segur | 01/04/2024 | 30/04/2024 | 17.000 € | 9 |
| **PROJ – 8** | Implementació de protecció criptogràfica de les dades | 15/04/2024 | 21/06/2024 | 42.000 € | 10 |
| **PROJ – 9** | Pla de continuïtat del negoci | 01/03/2024 | 29/03/2024 | 7.000 € | 6 |
| **PROJ – 10** | Implementació d'un sistema de gestió d'informació i esdeveniments de seguretat | 02/03/2024 | 13/06/2024 | 25.000 € | 7 |
| **Altres propostes** | | | | | |
| **PROJ – 11** | Programa de millora de la seguretat física en les instal·lacions | 01/07/2024 | 30/07/2024 | 10.000 € | 12 |
| **PROJ – 12** | Programa de millora de la gestió de RRHH | 07/05/2024 | 31/05/2024 | 6.000 € | 11 |

Taula 45. Resum dels Projectes

Amb aquesta sèrie de projectes per a millorar el nivell de seguretat es busca disminuir el nivell de risc. Tot i que és complicat concretar com afectarà de manera exacta i precisa, si que es pot dir que aquestes propostes de projectes pretenen aproximar-se al nivell de risc residual plantejat en el punt 4.3 de l'Anàlisi de Riscos.

Per tant, les propostes de projectes van alineades amb una anàlisi de l'impacte sobre la seguretat. Això representa que la seva execució ens ha d'indicar com

evoluciona el risc i l'impacte de materialització, així com el nivell de compliment dels diferents controls de la norma ISO/IEC 27002. Amb tota probabilitat, l'objectiu ha d'anar evolucionant cap a un nivell de maduresa optimitzat respecte a l'anàlisi GAP inicial realitzat en el punt 2.2.

A continuació, s'indica de forma gràfica en un diagrama de radar l'evolució estimada dels diferents grups de controls i el seu compliment abans i després de la realització dels diferents projectes.

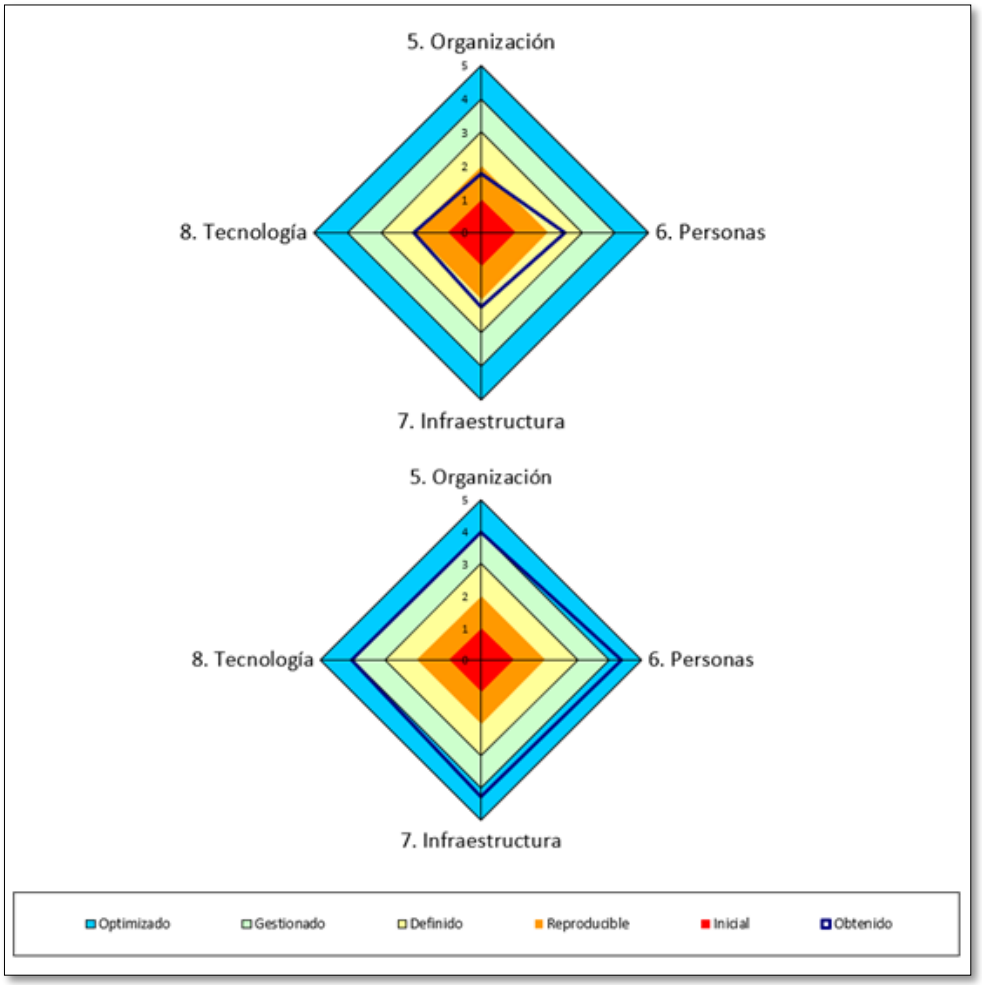


Figura 11. Comparativa GAP 27002 abans i després de les propostes de projectes.

S'ha de destacar que per conseqüència de la gran quantitat de controls que disposa la ISO 27002:2023, hi ha molts procediments que s'han d'implementar correctament per primera vegada a la cooperativa. Per aquesta raó, es considera apropiat assignar el valor de maduresa L4 – Gestionat i Mesurable, perquè necessitaria passar un període cíclic de millores continuades després d'implementar aquests projectes és podran millorar per arribar al grau d'optimització màxim.

# 6. Auditoria de Compliment

En aquesta etapa ja tenim gairebé acabada tota la implementació del SGSI, ja que els projectes anteriorment definits s'han implementat correctament. De manera que és necessari realitzar una auditoria que revisi els aspectes més rellevants en la cooperativa agrícola en matèria de seguretat, és a dir, el moment d'avaluar fins a quin punt l'empresa compleix amb les bones pràctiques.

L'ISO/IEC 27001 i 27002 (2023) servirà com a marc de control de l'estat actual de la seguretat amb la finalitat de mantenir el sistema de millora continua que estableix el SGSI. Aquesta auditoria de compliment és de tipus interna, i serà sobre la correcta implementació de la normativa ISO/IEC 27001:2023. Això representa la necessitat d'avaluar de nou la maduresa de la norma i dels controls per poder analitzar i estudiar la seva evolució.

A més, per poder dur a terme aquesta auditoria de compliment, és seguiran els procediments establerts en el punt 3.2 Procediment d'auditories internes.

**Avaluació de la maduresa**

En l'Annex 4 es pot trobar tota l'avaluació completa, i en aquest apartat es mostra una taula que resumeix els resultats, primerament, de l'avaluació de la normativa ISO 27001:2023. En haver realitzat tot aquest projecte del SGSI ja hi ha intrínsecament una millora prou notòria dels dominis corresponents. La comparativa inicial/actual usa els valors de la Taula 2 del punt 2 i és la següent:

| 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 |

Taula 46. Comparativa de la maduresa inicial i final de la normativa

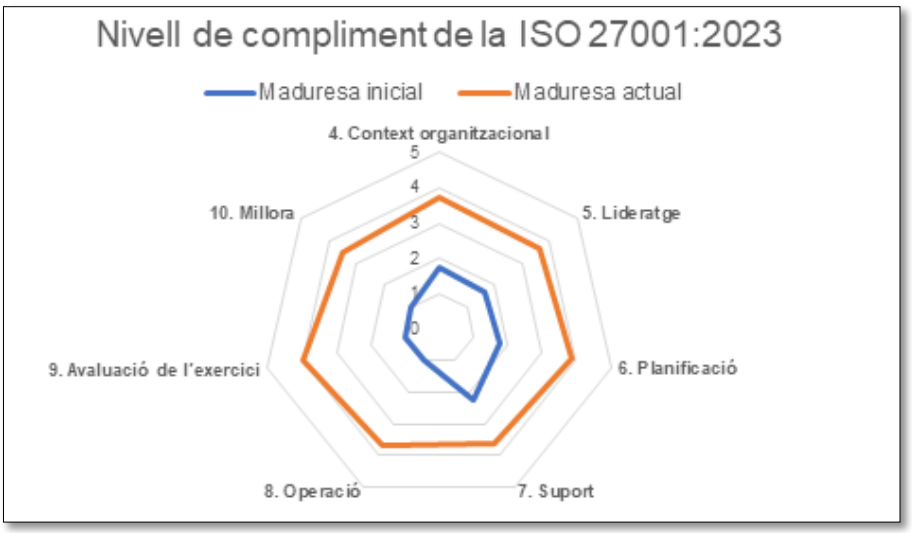


Figura 12. Nivell de maduresa de la normativa aconseguit

D'altra banda, en la següent taula de l'ISO 27002:2023 es mostren de manera resumida els valors de maduresa assolits dels quatre dominis de control.

| Dominis dels controls ISO 27002:2023 | 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 |

Taula 47. Comparativa de la maduresa inicial i final dels controls

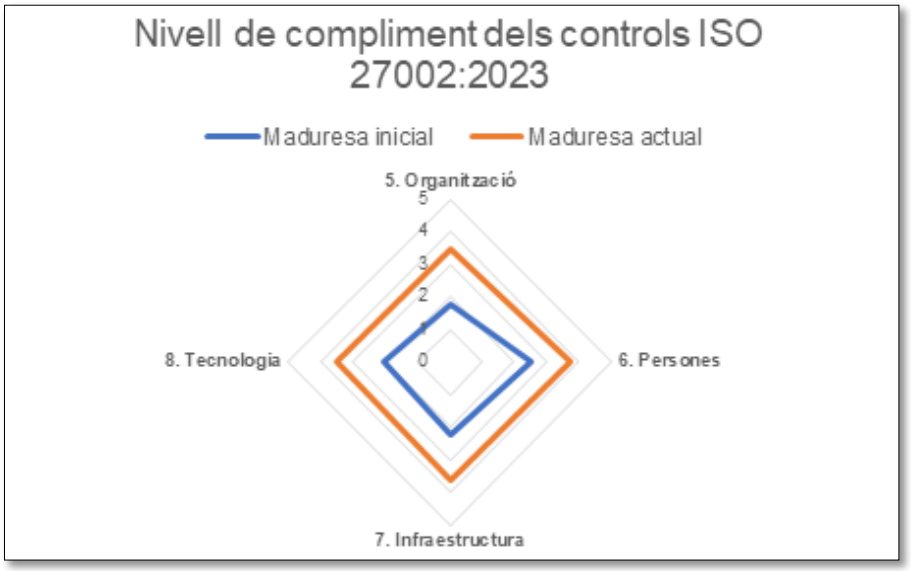


Figura 13. Nivell de maduresa dels controls aconseguit

## 6.1 Tasques i calendari d'execució

Les tasques de l'auditoria interna es detallen a continuació, amb l'abast de cadascuna, els actors necessaris i un calendari de proposta d'execució per un cicle de 3 anys.

**1. Definició del Pla d'Auditoria**

- **Abast:** Descripció de les ubicacions físiques, unitats organitzatives, activitats i processos; definició de les dates d'inici i finalització.
- **Actors:** Auditor Cap, Responsable del SGSI.
- **Durada:** 1 setmana.

**2. Revisió del sistema de gestió**

- **Abast:** Revisió de documentació del SGSI, context, abast, anàlisi i gestió del risc, declaració d'aplicabilitat (SOA), política de seguretat, rols de Seguretat, gestió de no conformitats, quadre de comandament.
- **Actors:** Auditor Cap, Equip Auditor, Responsable del SGSI, Responsables de les Àrees Auditades.
- **Durada:** 3 setmanes.

**3. Proves de compliment**

- **Abast:** Entrevistes amb propietaris d'actius, responsables de processos de negoci, usuaris del SGSI; revisió d'àrees de risc, comprovació d'objectius i metes establertes, revisió in situ de documentació.
- **Actors**: Auditor Cap, Equip Auditor, Responsable del SGSI, Propietaris d'Actius, Responsables de Processos de Negoci.
- **Durada:** 2 setmanes.

**4. Recollida i anàlisi de les evidències**

- **Abast:** Recollida de documents i dades necessàries per comprovar el compliment dels controls.
- **Actors:** Auditor Cap, Equip Auditor, Responsable del SGSI.
- **Durada:** 2 setmanes.

**5. Elaboració de l'informe d'auditoria**

- **Abast:** Redacció de l'informe amb resultats, no conformitats, observacions, punts forts, àrees de millora, accions correctives proposades, recomanacions.
- **Actors:** Auditor Cap, Equip Auditor, Responsable del SGSI.
- **Durada:** 1 setmana.

**6. Presentació dels resultats**

- **Abast:** Presentació de l'informe a la Direcció, àrees auditades i Comitè de Seguretat.
- **Actors:** Auditor Cap, Responsable del SGSI, Direcció, Responsables de les Àrees Auditades, Comitè de Seguretat.
- **Durada:** 1 setmana.

**7. Seguiment i implementació d'accions correctives**

- **Abast:** Establiment d'accions de seguiment, comprovació de l'eficàcia de les accions correctives.
- **Actors:** Responsable del SGSI, Equips de les Àrees Auditades.
- **Durada:** 8 setmanes.

Aquest és el calendari de l'auditoria de compliment. Com és pot veure, en cada anys es revisaria la normativa 27001, no obstant això, donada la càrrega de treball que implica fer una revisió total anualment, es proposa fer un cicle complet cada tres anys dels controls auditats.

| Normativa ISO/IEC 27001:2023 | Any 1 | Any 2 | Any 3 |
|---|---|---|---|
| 4. Context organitzacional | | | |
| 5. Lideratge | | | |
| 6. Planificació | | | |
| 7. Suport | | | |
| 8. Operació | | | |
| 9. Avaluació de l'exercici | | | |
| **Dominis dels controls ISO/IEC 27002:2023** | | | |
| 5. Organització | | | |
| 6. Persones | | | |
| 7. Infraestructura | | | |
| 8. Tecnologia | | | |

## 6.2 Anàlisi i interpretació de resultats

L'avaluació de la maduresa mostra una evolució significativa en totes les àrees avaluades. Inicialment, la majoria de les mesures de la normativa ISO 27001 i dels controls de l'ISO 27002 es trobaven en un estat inicial, amb una maduresa al nivell L1/L2, on els processos depenien principalment dels esforços individuals. No hi havia una estructura formalitzada ni una documentació adequada per gestionar la seguretat de la informació.

Després de la implementació dels projectes de millora, es pot observar un avenç considerable cap a nivells de maduresa més elevats. La maduresa actual s'ha situat majoritàriament en el nivell L3, indicant que els processos i els controls ara estan definits, documentats i comunicats adequadament. Això significa que s'ha assolit certa estructura formal per gestionar la seguretat de la informació, amb procediments estandarditzats i una major participació de tota l'organització en els processos de seguretat.

Això no obstant, no s'ha assolit el grau de maduresa objectiu excepte en una mesura. Aquests resultats representen que l'empresa es troba encara en possibilitats de millora, i és un escenari molt lògic i realista tenint en compte que s'ha implementat de 0 el SGSI, i que participa en la seva primera auditoria de compliment. Aleshores, gràcies a la metodologia PDCA el nivell de maduresa i compliment pujarà amb una futura revisió.

Finalment, encara que no s'han detectat motius que impliquin una no conformitat molt considerable, sí que s'han detectat alguns aspectes que podrien millorar-se o corregir-se. Les valors s'estableixen segons els següents criteris: No conformitat major / Menor / Observació / Oportunitat de millora.

| Sec. | Mesura o Control | Tipus | Comentari |
|---|---|---|---|
| | **Normativa ISO/IEC 27001:2023** | | |
| 4.3 | Determinar i documentar l'abast del SGSI | Oportunitat de millora | Es recomana revisar i millorar la documentació de l'abast del SGSI per assegurar la seva precisió i integritat. Podria definir-se més l'abast en relació a les activitats realitzades pels proveïdors i/o organitzacions afiliades. |
| 5.1 | La alta direcció ha de demostrar lideratge i compromís en relació con el SGSI. | Oportunitat de millora | Encara que s'han fet progressos, i el compromís ha millorat (sobretot en la creació del Comitè de Seguretat), es pot reforçar encara més el lideratge i l'assistència en les reunions per millorar la imatge i motivació. |

| | | | |
|---|---|---|---|
| 7.4 | Determinar la necessitat per a les comunicacions internes i externes rellevants a l'SGSI | Observació | Tot i que existeixen canals de comunicació, es poden millorar per assegurar que la informació rellevant sobre la seguretat de la informació arribi a tots els empleats i parts interessades de manera més efectiva i oportuna. Per exemple, els correus informatius sobre seguretat no son llegits per tot el personal de manera consistent (ja que no tothom revisa diàriament el seu correu), la qual cosa fa que alguns empleats no estiguin al corrent de les últimes polítiques i procediments de seguretat. |
| 7.5 | Informació documentada | Observació | La cooperativa i especialment el Comitè de Seguretat ha d'assegurar-se que la informació documentada arribi sempre en els terminis estipulats, assegurant-se que estigui a temps dels terminis estipulats per millorar l'eficàcia de tots els processos. |
| 8.1 | Planificar, implementar, controlar i documentar el procés de l'SGSI per gestionar els riscos. | No conformitat menor | Alguns riscos identificats no estan adequadament documentats un pla de tractament de riscos, cosa que pot portar a futurs problemes si no es corregeix. |
| | **Controls ISO/IEC 27002:2023** | | |
| 5.13 | Etiquetatge de la informació | No conformitat menor | Els processos per etiquetar la informació segons el seu nivell de sensibilitat no són consistents. |
| 5.24 | Planificació i preparació de la gestió d'incidents de seguretat d'informació | Observació | Si bé hi ha un SIEM i programes de conscienciació per als incidents, podria millorar-se mitjançant l'establiment de procediments més concrets durant l'experiència i el pas del temps per a la preparació i planificació prèvia a incidents. |
| 7.7 | Política de lloc de treball clar i pantalla neta | No conformitat menor | Hi ha mancances en l'aplicació de la política de neteja del lloc de treball i pantalla, posant en risc la seguretat de la informació i la privacitat dels empleats. |
| 7.14 | Eliminació o reutilització segura d'equips | No conformitat menor | Els processos per a la eliminació o reutilització d'equips no compleixen totalment amb els estàndards de seguretat, augmentant el risc de filtracions de dades. |
| 8.5 | Autenticació segura | Observació | Malgrat la implementació d'autenticació segura, es podria considerar l'ús de mètodes d'autenticació biomètrica per als treballadors que accedeixen a sistemes crítics de la planta de processament. Aquesta mesura podria millorar encara més la seguretat dels sistemes |
| 8.23 | Filtrat de webs | Oportunitat de millora | Podria ser beneficiós implementar un sistema que limiti l'accés a webs no relacionades amb les activitats agrícoles o empresarials, assegurant-se que els treballadors mantinguin el focus en les tasques essencials i minimitzin les distraccions durant les hores de treball. |
| 8.33 | Dades de prova | Observació | Es podria millorar la gestió de les dades de prova per assegurar que siguin adequades i completament anònimes per protegir la privacitat, especialment, de les dades personals. |

Taula 48. No conformitats de l'auditoria de compliment

# 7. Conclusions

Fer aquest treball sobre la implementació del SGSI en una cooperativa agrícola fictícia ha estat un procés enriquidor però sobretot bastant desafiador. Al llarg d'aquest treball, he donat context a aquesta empresa i durant aquest apartat he vist com mai la importància d'adoptar una metodologia estructurada, com la proporcionada per la norma ISO/IEC 27001, per garantir una gestió eficaç de la seguretat de la informació.

Durant el desenvolupament del TFM, s'ha posat de manifest la complexitat d'aquesta tasca, especialment tenint en compte que tant aquesta empresa com pràcticament qualsevol altra seria treballar sobre un entorn amb recursos limitats. Malgrat els obstacles trobats, considero que s'han assolit importants avenços en termes de seguretat de la informació, i destacaria especialment aquest cas, que és el d'una empresa que no tenia cap mena de mesura de seguretat de la informació prèvia, i el fet de poder generar una anàlisi de riscos emergeix com a recurs fonamental per a una posterior presa de decisions ben informada.

A més, mentre anava documentant-me i avançant amb les entregues, he pogut observar com la implementació d'un SGSI no sembla ser només una qüestió tècnica per a l'empresa, sinó també una qüestió estratègica per a l'organització, ja que requereix molta participació de tots els sectors i compromís amb la direcció. Per sort, s'ha decidit que per fer aquest treball la direcció de la cooperativa tingui una visió clara amb la protecció de la informació sensible, sent conscients dels beneficis que això aporta en termes de confiança i eficiència operativa.

Pel que respecta als objectius del treball, penso que s'han aconseguit importants avenços, i crec que sent realistes, els objectius es poden donar per assolits. Això no obstant, reconec que encara hi ha àrees de millora i reptes pendents, com ara la correcta i eficient consolidació dels controls de seguretat i la continuïtat dels esforços de millora continuada. Tant la direcció general com el personal del Comitè de Seguretat estan en el camí correcte per establir un entorn de treball segur i confiable, que els hi atorgui prestigi i confiança.

Finalment, vull esmentar l'aprenentatge adquirit durant aquest Treball Final de Màster. Ha estat una experiència molt enriquidora que m'ha proporcionat una comprensió més profunda sobre la importància de la seguretat de la informació i sobre la implementació d'un SGSI. Hi ha una gran diferència respecte al marc teòric que ja havia cursat en assignatures prèvies, i l'experiència adquirida m'ajudarà a poder col·laborar de manera professional en l'àrea de la gestió de la informació.

# Glossari

**PDS (Pla Director de Seguretat):** Document que estableix polítiques i procediments per gestionar la seguretat de la informació a llarg termini.

**SGSI (Sistema de Gestió de la Seguretat de la Informació):** Conjunt d'estructures i polítiques per protegir i gestionar sistemàticament la seguretat de la informació.

**ISO (International Organization for Standardization):** Organització que desenvolupa estàndards tècnics, incloent-hi ISO/IEC 27001 per la seguretat de la informació.

**IEC (Comissió Electrotècnica Internacional):** Organització que desenvolupa estàndards tècnics per l'electrotècnia i la tecnologia de la informació.

**PDCA (Cicle de Deming):** Cicle d'activitats de millora contínua: Planificar, Fer, Comprovar, Actuar.

**CMM (Capability Maturity Model):** Model per avaluar el nivell de maduresa dels processos en una organització.

**SoA (Statement of Applicability):** Document que identifica controls de seguretat per a la implementació en un SGSI.

**MAGERIT (Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes de Informació):** Metodologia per avaluar i gestionar riscos de seguretat de la informació.

**MAP (Ministeri d'Administracions Públiques):** Ministeri relacionat amb regulacions de seguretat de la informació en el sector públic.

**ENS (Esquema Nacional de Seguretat):** Polítiques i requisits de seguretat aplicats en el sector públic.

**KPI (Indicador Clau de Rendiment):** Mesura utilitzada per avaluar l'èxit d'un projecte o procés.

**SIEM (Security Information and Event Management):** Plataforma per recopilar i analitzar informació de seguretat.

# Annex 1. Bibliografia


Normalización Española. (2023). UNE-EN ISO/IEC 27001

Normalización Española. (2023). UNE-EN ISO/IEC 27002

MAGERIT (octubre de 2012). Portal de la Administración Electrónica.

Fresno, J.M. [José Manuel]. (6 de gener, 2024). Ciberseguridad en la industria agroalimentària. *ARTICA* [en línia].

Vige, W. [Whitney]. (14 de febrer, 2024). Mitigación de riesgos: cómo proteger a tu empresa en tiempos de cambio. ASANA [en línia]. https://asana.com/es/resources/risk-mitigation

INCIBE. (20 de juny de 2023). Instituto Nacional de Ciberseguridad. Obtingut de: Roles en ciberseguridad: desde el CEO a los usuarios finales: https://www.incibe.es/empresas/blog/roles-en-ciberseguridad-desde-el-ceo-los-usuarios-finales

CRUZ ALLENDE, Daniel. TORTAJADA GALLEGO, Arsenio. SEGOVIA HENARES, Antonio José. *Anàlisi de riscos* [en línia]. Barcelona: UOC. Disponible a: M1.709 – Sistemes de gestió de la seguretat. PID_00275340

GARRE GUI, Silvia. TORTAJADA GALLEGO, Arsenio. SEGOVIA HENARES, Antonio José. *Implantació d'un sistema de gestió de la seguretat de la informació (SGSI)* [en línia]. Barcelona: UOC. Disponible a: M1.709 – Sistemes de gestió de la seguretat. PID_00275344

GARRE GUI, Silvia. TORTAJADA GALLEGO, Arsenio. SEGOVIA HENARES, Antonio José. *Desenvolupament d'alguns objectius de control de l'SGSI* [en línia]. Barcelona: UOC. Disponible a: M1.709 – Sistemes de gestió de la seguretat. PID_00275342

ESTEVAN DE QUESADA, Rafael. *Auditoria tècnica de seguretat de sistemes d'informació i comunicacions* [en línia]. Barcelona: UOC. Disponible a: M1.710 - Auditoria tècnica. PID_00285940

# Annex 2. Anàlisi GAP

| Secció | Control | Nivell maduresa | Valor CMM | Valor mitjà | Justificació del nivell de madures del control |
|---|---|---|---|---|---|
| **5** | **Organització** | | | **1,756** | |
| **5.1** | Polítiques de seguretat de la informació | 2 - Repetible | 2 | | No hi ha polítiques específiques establertes però en el cas de la cooperativa assumeixo que les genèriques estan a l'ordre del dia (acords de confidencialitat, la seguretat física en la Planta de processament entre altres). Però hi ha una clara inexistència de determinades polítiques com ara la del teletreball, els ordinadors de les oficines, etc. Per la qual cosa, la fase inicial. Per la qual cosa, no hi ha plantilles definides a nivell corporatiu. |
| **5.2** | Rols i responsabilitats en seguretat de la informació | 2 - Repetible | 2 | | Encara que hi ha una estructura clara de les àrees específiques i un organigrama, hi falta documentació detallada de les responsabilitats de seguretat per a cada rol. Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca, i es normalitzen les bones pràctiques en base a l'experiència i al mètode. |
| **5.3** | Segregació de tasques | 3 - Definit | 3 | | L'empresa té una clara segregació de tasques però es podria millorar. D'aquesta manera, hi hauria menys conflictes i es reduirien els riscos de pèrdua d'informació. Si fos més alta, la protecció dels actius crítics seria més alta. |
| **5.4** | Responsabilitats de la direcció | 1 - Inicial | 1 | | La direcció general té compromís amb la seguretat de la informació i vol millorar-la. Però la presidència no hi està molt enterrada i podria tenir les responsabilitats més clares i específiques, així com la definició de metes amb major precisió. A més, no hi ha gaire comunicació entre el president i la direcció general. |
| **5.5** | Contacte amb les autoritats | 1 - Inicial | 1 | | En ser una empresa del sector de la producció i el comerç, tenen que tenir una bona relació amb les autoritats, especialment per les amenaces que poden sofrir. Però faria falta començar a detallar i formalitzar més els protocols específics en relació amb aquest control perquè no està detallat. |
| **5.6** | Contacte amb grups d'informació especials | 1 - Inicial | 1 | | Hi ha manca de protocols i processos formalitzats per a gestionar aquest contacte amb grups especials d'informació. Però són conscients de què ho necessiten. |
| **5.7** | Intel·ligència d'amenaces | 1 - Inicial | 1 | | Podrien identificar processos bàsics, com ara la pèrdua clara d'informació o atacs rebuts a causa de les conseqüències. Però no tenen una maduresa suficient com per afrontar les amenaces actuals. |
| **5.8** | Seguretat de la informació en la gestió de projectes | 1 - Inicial | 1 | | Fins ara, no s'ha proporcionat informació que mostri una implementació avançada d'aquest control en la gestió de projectes. Solament tenen antivirus en els portàtils i la resta està desprotegit. |
| **5.9** | Inventari d'informació i altres actius associats | 3 - Definit | 3 | | L'empresa té tot el personal definit, la informació gestionada (que mostra les dades més importants) i també té diagrames d'infraestructura i arquitectura on es detallen la resta d'actius. |
| **5.10** | Ús acceptable de la informació i actius associats | 2 - Repetible | 2 | | Tot i estar prou definit. La informació no rep un ús acceptable ja que està vulnerable en tot moment i no hi ha una fortificació sòlida. |
| **5.11** | Devolució d'actius | 1 - Inicial | 1 | | No hi ha una política de lliurament de dispositius mòbils i teletreball, i els ordinadors estan sense normalitzar ni xifrar. |

| | | | | | |
|---|---|---|---|---|---|
| **5.12** | Classificació de la informació | 3 - Definit | 3 | | L'empresa té clar quina informació consideren la més important, i de la mateixa manera, queda tot classificat amb una llista i ben vist. |
| **5.13** | Etiquetatge de la informació | 1 - Inicial | 1 | | No tenen un etiquetatge de la informació. Però no hi ha graus de confidencialitat o similars en cap de les llistes. |
| **5.14** | Transferència de la informació | 2 - Repetible | 2 | | La informació es transfereix constantment en una empresa com aquesta. Utilitzen Microsoft per a comunicar-se entre treballadors i també el SAP com a ERP. A més, disposen d'un túnel VPN amb autentificació, carpetes compartides. |
| **5.15** | Control d'accés | 3 - Definit | 3 | | Tenint en compte els escenaris i el tipus d'actius que hi ha en cada planta de la infraestructura, el control d'accés està gestionat mitjançant una subcontractació. Tenen càmeres de seguretat en la planta i disposen de control d'accés físic. |
| **5.16** | Gestió d'identitat | 3 - Definit | 3 | | En primer lloc, Microsoft 365 s'usa per gestionar la identitat dels treballadors (Azure AD), i amb la VPN les identitats locals. A més, de nou, suposarem que els treballadors que treballen a fora de l'empresa necessiten tenir un bon control d'identitat perquè hi hagi garantia de que son les persones autoritzades a tenir accés. De totes maneres, no hi ha més especificacions en el document, així que també podria ser més baix. |
| **5.17** | Informació d'autenticació | 2 - Repetible | 2 | | No hi ha polítiques implementades ni informació addicional sobre l'autenticació, però tenint en compte el mètode de carpetes compartides, i que utilitzen un ERP per a gestionar. |
| **5.18** | Drets d'accés | 2 - Repetible | 2 | | Considerant el que he dit prèviament i que són pràctiques en entorns híbrids, la gestió de la seguretat física ho controla l'empresa subcontractada (la que controla els accessos i vigila les instal·lacions.) |
| **5.19** | Seguretat de la informació en les relacions amb els proveïdors | 3 - Definit | 3 | | La cooperativa te una gran quantitat de socis, especialment en el sector agrícola e industrial. Per la qual cosa, hi ha processos definits i documentats, i a la cooperativa ja tenen certa estructura i processos establerts amb els proveïdors externs. |
| **5.20** | Abordar la seguretat de la informació dins dels acords de proveïdors | 2 - Repetible | 2 | | És probable que ja hagin establert algunes clàusules de seguretat en els acords amb els proveïdors ja que tenen la seva confiança. |
| **5.21** | Gestió de la seguretat de la informació a la cadena de subministrament de les TIC | 1 - Inicial | 1 | | Volem implantar un SGSI per tenir la seguretat de la informació coberta. Com tenen una àrea T.I, seria recomanable produir una de seguretat a part. Això no obstant, no han rebut pèrdues significatives al llarg dels anys i sembla que han aconseguit cobrir els aspectes més bàsics. |
| **5.22** | Seguiment, revisió i gestió del canvi dels serveis de proveïdors | 3 - Definit | 3 | | La cooperativa es manté actualitzada amb aquest control. Els departaments administratius i la junta directiva (amb el president) estan a l'ordre del dia. |
| **5.23** | Seguretat de la informació per a l'ús de serveis al núvol | 1 - Inicial | 1 | | Es pràcticament nul, això no obstant, son coneixedors d'aquest problema, i fins ara, solament utilitzen Azure per a identificar els treballadors a les aplicacions corporatives |
| **5.24** | Planificació i preparació de la gestió d'incidents de seguretat d'informació | 2 - Repetible | 2 | | Donat que l'empresa es troba en un sector crític i ha manifestat la intenció de posicionar-se al mercat garantint la seguretat dels seus serveis, podríem considerar un nivell de maduresa més alt que no pas el no existeix. La justificació està en la importància d'una resposta estructurada davant d'incidents de seguretat en un context on els ciberatacs en aquest sector són en augment. |

| | | | | | |
|---|---|---|---|---|---|
| **5.25** | Avaluació i decisió sobre els esdeveniments de seguretat d'informació | 1 - Inicial | 1 | | Pràcticament està començant a requerir d'aquests avaluacions, per tant, l'únic que ens queda amb aquest context es que son conscients de que han de contemplar la seguretat però no tenen res més que plantejaments |
| **5.26** | Resposta a incidents de seguretat de la informació | 1 - Inicial | 1 | | Estan en procés d'aprenentatge, per tant, l'únic que ens queda amb aquest context es que son conscients de que han de contemplar la seguretat però no tenen res més que plantejaments |
| **5.27** | Aprenentatge dels incidents de seguretat de la informació | 1 - Inicial | 1 | | En la situació actual estan aprenent, per tant, l'únic que ens queda amb aquest context es que son conscients de que han de contemplar la seguretat però no tenen res més que plantejaments |
| **5.28** | Recull d'evidències | 1 - Inicial | 1 | | Són conscients de la situació emergent que estan vivint però necessiten d'un equip amb coneixements per recollir bé les evidències. |
| **5.29** | Seguretat de la informació durant la interrupció | 1 - Inicial | 1 | | La informació no destaca clarament procediments o plans concrets per gestionar la seguretat de la informació durant interrupcions. Potser hi ha una consciència general d'aquesta necessitat, però no hi ha un enfocament estructurat o documentat en el context actual. |
| **5.30** | Preparació per a les TIC per a la continuïtat del negoci | 1 - Inicial | 1 | | No es destaquen mesures específiques per garantir la continuïtat en casos de fallades en aquesta ubicació. Però es reconeix el problema. |
| **5.31** | Identificació de requisits legals, reglamentaris i contractuals | 3 - Definit | 3 | | S'indica una consciència de la importància de la seguretat, com ara la inclusió d'acords de confidencialitat en els contractes laborals. També esmenta contractes amb clients, indicant una consideració de requisits contractuals. |
| **5.32** | Drets de propietat intel·lectual (DPI) | 2 - Repetible | 2 | | Tenint en compte el Marc Legal de l'empresa, els drets DPI podrien estar inclosos la documentació i assumeixo que tot i no ser un aspecte important del sector de producció d'aliments, és intuïtiu. |
| **5.33** | Protecció dels registres de l'organització | 2 - Repetible | 2 | | La importància dels registres de recanvis de maquinari, de logística, dels empleats i de les dades de producció es tan gran que suggereix que hi ha un conjunt divers de registres essencials per a les operacions i la presa de decisions de l'organització i la protecció d'aquests la tenen en compte tot i que els errors són probables. |
| **5.34** | Privadesa i protecció de la informació d'identificació personal | 2 - Repetible | 2 | | Pràcticament està començant a requerir d'aquests avaluacions, per tant, l'únic que ens queda amb aquest context es que son conscients de que han de contemplar la seguretat però no tenen gairebé res i poden haver-hi moltes fugues. |
| **5.35** | Revisió independent de la seguretat de la informació | 1 - Inicial | 1 | | No s'esmenta cap control de backups o revisió en general, això no obstant, l'equip I.T deu tenir-ho en planificació inicial. |
| **5.36** | Compliment de les polítiques i normes de seguretat de la informació | 2 - Repetible | 2 | | L'equip I.T de la cooperativa estableixen directrius bàsiques a tots els treballadors i cadascú es fa responsable en base a la seva pròpia experiència. |
| **5.37** | Documentació de procediments d'operació | 1 - Inicial | 1 | | No hi ha cap mena de polítiques ni compliment perquè estan en un punt de partida amb aquest sector. |
| **6** | **Persones** | | | **2,5** | |
| **6.1** | Comprovació | 2 - Repetible | 2 | | La cooperativa es una empresa molt important en el sector agrícola del territori. La complexitat dels seus serveis fa que importància de garantir que es compleixen les polítiques i les normes de seguretat ha de tenir un bon nivell de comprovació. |

| | | | | | |
|---|---|---|---|---|---|
| **6.2** | Termes i condicions de contractació | 3 - Definit | 3 | | L'àrea de finances i de recursos humans s'encarreguen dels termes i de la contractació, així com de l'apartat legal i fiscal de l'empresa. |
| **6.3** | Conscienciació, educació i formació en seguretat de la informació | 2 - Repetible | 2 | | La direcció general està convençuda d'invertir en ciberseguretat, i per això vol començar amb la implantació d'un SGSI. El fet de que el "cap" estigui conscienciat, facilita que tota l'empresa ho acabi fent. |
| **6.4** | Procés disciplinari | 2 - Repetible | 2 | | L'àrea de RRHH s'encarrega des aspectes de formació, i tot i que no existeixi un procediment per si mateix, tots els usuaris semblen ser responsables. Però els errors son molt probables. |
| **6.5** | Responsabilitat davant la finalització o canvi | 3 - Definit | 3 | | Suposarem que cada membre de l'empresa es fa responsable per si mateix en cas de finalització o canvi pel context proporcionat. |
| **6.6** | Acords de confidencialitat o no divulgació | 3 - Definit | 3 | | Podríem considerar-ho perquè el marc legal de l'empresa està actualitzat d'acord a la protecció de dades en l'àmbit Europeu. |
| **6.7** | Treball en remot | 3 - Definit | 3 | | Permet treballar en remot, per tant hi ha una modalitat híbrida per als empleats i podríem considerar-ho prou definit. (A més s'usa un VPN) |
| **6.8** | Notificació dels esdeveniments de seguretat de la informació | 2 - Repetible | 2 | | L'equip I.T s'encarregava fins ara d'aquest sector, però ara es quan estem començant a invertir en el SGSI. |
| **7** | **Infraestructura** | | | **2,214** | |
| **7.1** | Perímetre de seguretat física | 3 - Definit | **3** | | La gestió de la seguretat física està subcontractada a una empresa de seguretat que controla els accessos i vigila les instal·lacions. Això no obstant, no es disposa de tecnologia per automatitzar el flux de treball i es podria millorar la qualitat i l'eficiència. |
| **7.2** | Controls físics d'entrada | 3 - Definit | **3** | | La gestió de la seguretat física està subcontractada a una empresa de seguretat que controla els accessos i vigila les instal·lacions. Això no obstant, no es disposa de tecnologia per automatitzar el flux de treball i es podria millorar la qualitat i l'eficiència. |
| **7.3** | Seguretat d'oficines, despatxos i recursos | 3 - Definit | **3** | | La gestió de la seguretat física està subcontractada a una empresa de seguretat que controla els accessos i vigila les instal·lacions. Això no obstant, no es disposa de tecnologia per automatitzar el flux de treball i es podria millorar la qualitat i l'eficiència. |
| **7.4** | Vigilància de la seguretat física | 3 - Definit | **3** | | La gestió de la seguretat física està subcontractada a una empresa de seguretat que controla els accessos i vigila les instal·lacions. Això no obstant, no es disposa de tecnologia per automatitzar el flux de treball i es podria millorar la qualitat i l'eficiència. |
| **7.5** | Protecció contra les amenaces externes i ambientals | 1 - Inicial | **1** | | No hi ha mesures específiques per protegir-se contra amenaces externes i ambientals. No s'ha mencionat cap acció o control específic en aquest sentit. Això no obstant, l'empresa subcontractada podria tenir-ho en compte |
| **7.6** | El treball en àrees segures | 3 - Definit | **3** | | Amb la informació proporcionada, decideixo classificar-lo d'aquesta manera perquè tinc en compte que l'empresa té la pròpia planta de processament de l'arròs on només els treballadors formats en aquell sector tenen accés a l'espai. Utilitzen restricció d'accés a personal autoritzat, l'ús de sistemes de monitoratge, la formació del personal i l'establiment de procediments per a situacions d'emergència. |
| **7.7** | Política de lloc de treball clar i | 2 - Repetible | **2** | | Tot i no haver una política clara i definida, és normalitzen les bones pràctiques en base a |

| | | | | | |
|---|---|---|---|---|---|
| | pantalla neta | | | | l'experiència dels treballadors i aquests son veterans en ser una empresa "vella". Per tant, podria dependre de cada usuari la instal·lació i configuració de cada equip de treball. |
| **7.8** | Emplaçament i protecció d'equips | 2 - Repetible | **2** | | Tot i no haver una política clara i definida, és normalitzen les bones pràctiques en base a l'experiència dels treballadors i aquests son veterans en ser una empresa "vella". Per tant, podria dependre de cada usuari la instal·lació i configuració de cada equip de treball. |
| **7.9** | Seguretat dels equips fora de les instal·lacions | 2 - Repetible | **2** | | Tot i no haver una política clara i definida, és normalitzen les bones pràctiques en base a l'experiència dels treballadors i aquests son veterans en ser una empresa "vella". Per tant, podria dependre de cada usuari la instal·lació i configuració de cada equip de treball. |
| **7.10** | Mitjans d'emmagatzematge | 2 - Repetible | **2** | | L'equip I.T s'encarrega d'aquest control, però no s'ha definit cap política de còpia periòdica o setmanal de les BBDD. Això es molt feixuc i l'empres necessita canvis durant la planificació del SGSI. |
| **7.11** | Instal·lacions de subministrament | 3 - Definit | **3** | | En la planta de producció s'encarreguen de mantenir tot el maquinari respost, així com qualsevol recanvi possible. |
| **7.12** | Seguretat del cablejat | 1 - Inicial | **1** | | No existeix cap control d'aquest tipus en el document ni sembla que hi hagi cap possible deducció. Això no obstant, el departament I.T pot tenir-ho com a fase inicial. |
| **7.13** | Manteniment dels equips | 2 - Repetible | **2** | | No hi ha cap política per als portàtils o similars pel que respecta a això. Com deia anteriorment, cada empleat es fa càrrec a voluntat pròpia de la seva àrea de treball, però s'hauria de definir i clarificar. De la mateixa manera, succeeix amb el maquinari de producció. |
| **7.14** | Eliminació o reutilització segura d'equips | 1 - Inicial | **1** | | No existeix cap control d'aquest tipus en el document ni sembla que hi hagi cap possible deducció. Però es reconeix el problema a resoldre. |
| **8** | **Tecnologia** | | | **2,029** | |
| **8.1** | Dispositius de punt final d'usuari | 1 - Inicial | **1** | | No existeix cap control d'aquest tipus en el document ni sembla que hi hagi cap possible deducció. Això no obstant, el departament I.T pot tenir-ho com a fase inicial per al maneig segur dels dispositius, el registre, etc. |
| **8.2** | Gestió de privilegis d'accés | 3 - Definit | **3** | | Solament s'usa Microsoft 365 per gestionar la identitat dels treballadors a les aplicacions corporatives i el router coma VPN amb autenticació d'identitats per contrasenya. El departament I.T maneja aquest control. |
| **8.3** | Restricció d'accés a la informació | 2 - Repetible | **2** | | La instal·lació i configuració dels equips de treball està definida per l'equip I.T però després els usuaris són els administradors locals dels seus equips. Això podria indicar que les restriccions d'accés a la informació no estan de manera estandarditzada i centralitzada, sinó que depenen de les pròpies eleccions i configuracions dels usuaris. |
| **8.4** | Accés al codi font dels programes | 2 - Repetible | **2** | | L'equip I.T no ha definit aquest control però hi ha formació en aquest departament i en haver-hi grau de coneixement segurament s'encarreguin durant la instal·lació i configuració dels equips. |
| **8.5** | Autenticació segura | 2 - Repetible | **2** | | L'equip I.T està format per encarregar-se mínimament de que els treballadors tinguin una autenticació prou correcta en l'accés dels programaris. |
| **8.6** | Gestió de capacitats | 1 - Inicial | **1** | | No existeix cap control d'aquest tipus en el document ni sembla que hi hagi cap possible |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | deducció. Això no obstant, el departament I.T pot tenir-ho com a fase inicial per al maneig segur dels dispositius, el registre, etc. |
| **8.7** | Controls contra el codi maliciós | 2 - Repetible | **2** | | L'equip I.T no ha definit aquest control però hi ha formació en aquest departament i en haver-hi grau de coneixement segurament s'encarreguin d'un control estandarditzat sobre el codi maliciós. |
| **8.8** | Gestió de vulnerabilitats tècniques | 2 - Repetible | **2** | | L'equip I.T no ha definit aquest control però hi ha formació en aquest departament i part de la seva feina es evitar l'explotació de vulnerabilitats en els seus programaris i entorn digital. |
| **8.9** | Gestió de la configuració | 3 - Definit | **3** | | L'àrea I.T gestiona la configuració, documenta, implementa, monitoritza i revisa el hardware, software, serveis i xarxa. La part on hi ha més falta de millora es en la configuració de seguretat. |
| **8.10** | Eliminació de la informació | 2 - Repetible | **2** | | L'equip I.T té la suficient formació com per entendre que la informació ha de desaparèixer dels medis que ja no es necessiten. Això no obstant, no hi ha una política clara i definida i es basa en cada persona. |
| **8.11** | Emmascarament de dades | 1 - Inicial | **1** | | No hi ha evidències de que l'empresa ho plantegi, però l'equip I.T ho deu tenir en fase inicial i es reconeix el problema. |
| **8.12** | Prevenció de fuites de dades | 2 - Repetible | **2** | | Hi ha un departament I.T que controla l'ús dels comptes, obliga a usar contrasenyes, Firewall, la xarxa VPN, etc. Hi fa falta una major dedicació a aquest control això no obstant. |
| **8.13** | Còpies de seguretat de la informació | 2 - Repetible | **2** | | El departament I.T és qui controla les còpies de seguretat. No obstant això, no tenen una política regular i estricta que ho dictamini. |
| **8.14** | Redundància de les instal·lacions de processament d'informació | 2 - Repetible | **2** | | Existeix un procediment per a la redundància dels recursos de tractament de la informació. |
| **8.15** | Registres | 2 - Repetible | **2** | | L'empresa pot tenir certa estructura en la creació i emmagatzematge de registres, però no és completament definit o estandarditzat. |
| **8.16** | Seguiment d'activitats | 3 - Definit | **3** | | Hi ha un seguiment prou exhaustiu de totes les activitats de l'empresa, especialment d'entrada i sortida, recanvis i gestió d'expedients i treballadors. |
| **8.17** | Sincronització del rellotge | 3 - Definit | **3** | | Els equips i servidors estan sincronitzats a una únic servidor. |
| **8.18** | Ús de les utilitats amb privilegis del sistema | 3 - Definit | **3** | | Existeixen procediments on es recullen les etapes d'implementació i posada en producció dels softwares desenvolupats per l'organització, les proves es realitzen en entorns aïllats i segurs |
| **8.19** | Instal·lació del programari en entorn de producció | 3 - Definit | **3** | | Existeixen procediments on es recullen les etapes d'implementació i posada en producció dels softwares desenvolupats per l'organització, les proves es realitzen en entorns aïllats i segurs |
| **8.20** | Controls de xarxa | 3 - Definit | **3** | | Es disposa d'una certa estructura i repetició en l'ús de controls de xarxa com la VPN, Firewall, identificació dels ports. Procediments d'alta i baixa dels usuaris treballadors. |
| **8.21** | Seguretat dels serveis de xarxa | 3 - Definit | **3** | | Es disposa d'una certa estructura i repetició en l'ús de controls de xarxa com la VPN, Firewall, identificació dels ports. Procediments d'alta i baixa dels usuaris treballadors. |
| **8.22** | Segregació en xarxes | 3 - Definit | **3** | | Es disposa d'una certa estructura i repetició en l'ús de controls de xarxa com la VPN, Firewall, identificació dels ports. Procediments d'alta i baixa dels usuaris treballadors. |
| **8.23** | Filtrat de webs | 0 - No existent | **0** | | Tenint en compte que els servidors no tenen protecció antimalware, que les dades dels sensors s'envien sense xifrar i veient com funcionen els backups (a més de que no s'esmenta textualment |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | aquest control), penso que no el tenen en compte. |
| **8.24** | Ús de la criptografia | 2 - Repetible | **2** | | Les plataformes web tenen un xifrat amb les comunicacions, però faria falta que l'equip I.T fes una normativa amb enviament de documents xifrats o protegits amb claus d'accés. |
| **8.25** | Seguretat en el cicle de vida dels desenvolupaments | 1 - Inicial | **1** | | El director general es conscient de la falta de seguretat i hi ha conscienciació, però actualment no hi ha aquest tipus de seguretat. |
| **8.26** | Requisits de seguretat de les aplicacions | 1 - Inicial | **1** | | Es disposa d'una certa estructura i repetició en l'ús de controls de xarxa com la VPN, Firewall, identificació dels ports. Procediments d'alta i baixa dels usuaris treballadors. |
| **8.27** | Arquitectura segura de sistemes i principis d'enginyeria | 2 - Repetible | **2** | | Es disposa d'una certa estructura i repetició en l'ús de controls de xarxa com la VPN, Firewall, identificació dels ports. Procediments d'alta i baixa dels usuaris treballadors. |
| **8.28** | Codificació segura | 1 - Inicial | **1** | | L'equip I.T està format i és conscient de la necessitat d'aplicar aquest control a curt termini. |
| **8.29** | Proves de seguretat en desenvolupament i acceptació | 3 - Definit | **3** | | Es té un procediment on es recullen les etapes d'implementació i la posada en producció del softwares desenvolupats i les proves es realitzen en entorns aïllats i segures |
| **8.30** | Externalització del desenvolupament de programari | 3 - Definit | **3** | | El desenvolupament de programari propi és intern i està subjecte al descrit en punts anteriors, en cas que s'internalitzés hauria de seguir els procediments establerts per l'organització |
| **8.31** | Separació dels recursos de desenvolupament, prova i operació | 3 - Definit | **3** | | Existeixen procediments on es recullen les etapes d'implementació i posada en producció dels softwares desenvolupats per l'organització, les proves es realitzen en entorns aïllats i segurs |
| **8.32** | Gestió de canvis | 1 - Inicial | **1** | | El director general es conscient de la falta de seguretat i hi ha conscienciació, però actualment no hi ha aquest tipus de gestió |
| **8.33** | Dades de prova | 1 - Inicial | **1** | | El director general es conscient de la falta de seguretat i hi ha conscienciació, però actualment no hi ha aquest tipus de gestió |
| **8.34** | Protecció dels sistemes d'informació durant l'auditoria i les proves | 1 - Inicial | **1** | | El director general es conscient de la falta de seguretat i hi ha conscienciació, però actualment no hi ha aquest tipus de gestió |

Taula 49. Declaració d'Aplicabilitat

# Annex 3. Declaració d'aplicabilitat

| Secció | Control | Aplica (Si/No) | Estat actual | Nivell de compliment | Comentaris |
|---|---|---|---|---|---|
| **5** | **Context de l'organització** | | | | |
| **5.1** | Polítiques de seguretat de la informació | Sí | En implementació | Mitjà | Les polítiques de seguretat de la informació estan sent desenvolupades i documentades, però encara no s'han implementat completament. Es requereixen més accions per a la seva aplicació total. |
| **5.2** | Rols i responsabilitats en seguretat de la informació | Sí | Implementat | Alt | Els rols i les responsabilitats en matèria de seguretat de la informació han estat definits i assignats de manera clara a tots els nivells de la cooperativa. |
| **5.3** | Segregació de tasques | Sí | Implementat | Alt | S'han identificat i implementat les polítiques de segregació de tasques per evitar la concentració excessiva de poder i reduir els riscos associats. |
| **5.4** | Responsabilitats de la direcció | Sí | En implementació | Mitjà | L'alta direcció ha mostrat compromís amb el sistema de gestió de la seguretat de la informació, però s'han de definir clarament les seves responsabilitats en aquest àmbit. |
| **5.5** | Contacte amb les autoritats | Sí | Implementat | Alt | La cooperativa ha establert protocols de contacte amb les autoritats pertinents en cas d'incidents de seguretat importants. |
| **5.6** | Contacte amb grups d'informació especials | Sí | En implementació | Mitjà | Es requereixen procediments més específics per al contacte amb grups especials d'informació en situacions de seguretat especials. |
| **5.7** | Intel·ligència d'amenaces | Sí | Implementat | Mitjà | La cooperativa manté un sistema de vigilància d'amenaces en temps real, però s'ha de millorar la seva eficàcia per a una detecció més proactiva. |
| **5.8** | Seguretat de la informació en la gestió de projectes | Sí | Implementat | Alt | Es garanteix que els riscos de seguretat de la informació relacionats amb els projectes són abordats de manera eficaç en la gestió de projectes al llarg de tot el seu cicle de vida. |
| **5.9** | Inventari d'informació i altres actius associats | Sí | En implementació | Mitjà | Es duu a terme una identificació inicial dels actius d'informació, però encara es requereix una revisió completa i una catalogació detallada dels mateixos. |
| **5.10** | Ús acceptable de la informació i actius associats | Sí | Implementat | Alt | La cooperativa garanteix que la informació i els actius associats es protegeixen, utilitzen i manegen adequadament d'acord amb les polítiques establertes. |
| **5.11** | Devolució d'actius | Sí | En implementació | Mitjà | Es requereixen procediments més específics per a la protecció dels actius de l'organització en el procés de devolució o finalització. |
| **5.12** | Classificació de la informació | Sí | Implementat | Mitjà | La cooperativa ha començat a classificar la informació d'acord amb les necessitats de seguretat, però aquest procés encara no està complet. |
| **5.13** | Etiquetatge de la informació | Sí | Implementat | Mitjà | S'han implementat procediments per etiquetar la informació, però encara hi ha algunes àrees on aquest procés no s'aplica de manera consistent. |
| **5.14** | Transferència de la informació | Sí | En implementació | Mitjà | Es requereixen procediments més clars i protocols per a la transferència segura de la informació tant dintre com fora de la cooperativa. |
| **5.15** | Control d'accés | Sí | Implementat | Alt | S'han establert i implementat regles de control d'accés físic i lògic a la informació i |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | altres actius associats d'acord amb els requisits establerts. |
| **5.16** | Gestió d'identitat | Sí | Implementat | Alt | Es gestiona de manera completa el cicle de vida de les identitats d'usuari per garantir la seva seguretat i integritat. |
| **5.17** | Informació d'autenticació | Sí | En implementació | Mitjà | Es requereix un procés formal de gestió de la informació d'autenticació, incloent l'assessorament al personal, per millorar la seguretat en aquest àmbit. |
| **5.18** | Drets d'accés | Sí | En implementació | Mitjà | S'han establert i aprovat els drets d'accés, però es requereix una revisió i actualització periòdiques per garantir la seva eficàcia contínua. |
| **5.19** | Seguretat de la informació en les relacions amb els proveïdors | Sí | En implementació | Mitjà | Es requereixen processos i procediments més detallats per gestionar els riscos de seguretat associats amb els proveïdors de la cooperativa. |
| **5.20** | Abordar la seguretat de la informació dins dels acords de proveïdors | Sí | Implementat | Mitjà | S'han establert i acordat requisits de seguretat amb els proveïdors, però s'han de revisar periòdicament per assegurar-ne el compliment. |
| **5.21** | Gestió de la seguretat de la informació a la cadena de subministrament de les TIC | Sí | En implementació | Mitjà | Es requereixen processos i procediments més detallats per fer front als riscos de seguretat de la informació associats amb la cadena de subministrament de les TIC. |
| **5.22** | Seguiment, revisió i gestió del canvi dels serveis de proveïdors | Sí | Implementat | Mitjà | Es realitzen supervisions i revisions periòdiques, però es requereix un enfocament més estructurat per gestionar els canvis als serveis dels proveïdors. |
| **5.23** | Seguretat de la informació per a l'ús de serveis al núvol | Sí | En implementació | Mitjà | Es requereixen procediments més específics per a l'adquisició, ús i gestió segura dels serveis al núvol d'acord amb els requisits de seguretat establerts. |
| **5.24** | Planificació i preparació de la gestió d'incidents de seguretat d'informació | Sí | En implementat | Mitjà | S'han establert plans i procediments per a la gestió d'incidents, però encara s'han de provar i comunicar a tot el personal. Cal revisar i actualitzar el procediment conforme les exigències de la ISO 27001. |
| **5.25** | Avaluació i decisió sobre els esdeveniments de seguretat d'informació | Sí | En implementació | Parcialment | Es requereix una millora en el procés d'avaluació i presa de decisions sobre els esdeveniments de seguretat per a una resposta més ràpida i eficaç. |
| **5.26** | Resposta a incidents de seguretat de la informació | Sí | En implementació | Mitjà | S'han definit els procediments de resposta a incidents, però encara es requereix entrenament i proves per a una execució eficient. |
| **5.27** | Aprenentatge dels incidents de seguretat de la informació | Sí | En implementació | Mitjà | Es requereixen procediments per quantificar i monitoritzar els incidents de seguretat per millorar els processos de prevenció i resposta. |
| **5.28** | Recull d'evidències | Sí | Implementat | Alt | S'han establert i implementat procediments per a la identificació, recollida i preservació d'evidències relacionades amb els incidents de seguretat. |
| **5.29** | Seguretat de la informació durant la interrupció | Sí | En implementació | Mitjà | Es requereix una planificació més detallada per mantenir la seguretat de la informació durant situacions d'interrupció. |
| **5.30** | Preparació per a les TIC per a | Sí | Implementat | Alt | S'han establert i implementat plans per garantir la continuïtat del negoci i de les |

| | | | | | |
|---|---|---|---|---|---|
| | la continuïtat del negoci | | | | TIC en cas d'interrupció. |
| **5.31** | Identificació de requisits legals, reglamentaris i contractuals | Sí | Implementat | Alt | Es manté un registre actualitzat dels requisits legals, reglamentaris i contractuals relatius a la seguretat de la informació i es compleixen de manera adequada. |
| **5.32** | Drets de propietat intel·lectual (DPI) | Sí | En implementació | Mitjà | Es requereixen més accions per a protegir de manera efectiva els drets de propietat intel·lectual associats amb la informació i els actius de la cooperativa. |
| **5.33** | Protecció dels registres de l'organització | Sí | Implementat | Mitjà | S'han implementat mesures per protegir els registres de l'organització contra pèrdua, destrucció, accés no autoritzat i divulgació no autoritzada. |
| **5.34** | Privadesa i protecció de la informació d'identificació personal | Sí | Implementat | Mitjà | Es requereixen més mesures per garantir el compliment de les lleis i regulacions relatives a la privades |
| **5.35** | Revisió independent de la seguretat de la informació | Si | En implementació | Mitjà | S'ha planificat fer una revisió independent de la seguretat de la informació, però encara no s'ha dut a terme. S'espera completar aquesta revisió els propers mesos per assegurar que l'enfocament de l'organització en la gestió de la seguretat de la informació sigui efectiu. |
| **5.36** | Compliment de les polítiques i normes de seguretat de la informació | Si | En implementació | Mitjà | Es fa una verificació periòdica del compliment amb la política de seguretat de la informació i les normes de l'organització. Tot i això, s'han identificat algunes àrees en què cal millorar el compliment, i s'estan implementant mesures correctives per abordar-les. |
| **5.37** | Documentació de procediments d'operació | Si | En implementació | Baix | S'estan documentant els procediments operatius dels mitjans de tractament de la informació, però encara no s'han posat a la disposició de tots els usuaris que els necessiten. S'espera completar aquest procés els propers mesos per millorar l'eficiència i la consistència en les operacions relacionades amb la seguretat de la informació. |
| **6** | **Persones** | | | | |
| **6.1** | Comprovació | Sí | En implementació | Mitjà | Es realitzen verificacions periòdiques però es requereix millorar els processos de comprovació per assegurar el compliment total de les polítiques. |
| **6.2** | Termes i condicions de contractació | Sí | Implementat | Alt | La cooperativa té subcontractats serveis de seguretat física. És crucial assegurar que els termes i condicions dels contractes amb aquests proveïdors incloguin disposicions específiques per garantir la protecció adequada de la informació i altres actius de la cooperativa. |
| **6.3** | Conscienciació, educació i formació en seguretat de la informació | Sí | En implementació | Mitjà | S'han realitzat sessions de formació inicial, però es necessita un programa de formació continuada per mantenir la conscienciació en seguretat. |
| **6.4** | Procés disciplinari | Sí | Implementat | Alt | S'han establert i comunicat els procediments disciplinaris per a incompliments de les polítiques de seguretat de la informació. |
| **6.5** | Responsabilitat davant la finalització o canvi | Sí | En implementació | Baix | Es requereix millorar la claredat de les responsabilitats davant finalització o canvi en relació amb la seguretat de la informació. |

| | | | | | |
|---|---|---|---|---|---|
| **6.6** | Acords de confidencialitat o no divulgació | Sí | Implementat | Alt | S'han signat acords de confidencialitat amb el personal relatiu a la seguretat de la informació i la seva divulgació. |
| **6.7** | Treball en remot | Sí | En implementació | Mitjà | Es requereixen mesures addicionals per garantir la seguretat de la informació en les tasques realitzades en un entorn de treball remot. |
| **6.8** | Notificació dels esdeveniments de seguretat de la informació | Sí | Implementat | Alt | S'han establert procediments per a la notificació ràpida dels esdeveniments de seguretat de la informació per permetre una resposta eficient i efectiva. |
| **7** | **Infraestructura** | | | | |
| **7.1** | Perímetre de seguretat física | Sí | En implementació | Mitjà | S'han instal·lat sistemes de control d'accés a les instal·lacions, però encara s'ha de millorar la monitorització i la vigilància. |
| **7.2** | Controls físics d'entrada | Sí | Implementat | Alt | S'han establert controls d'accés físic a totes les entrades de l'edifici i s'apliquen de manera eficaç. |
| **7.3** | Seguretat d'oficines, despatxos i recursos | Sí | En implementació | Mitjà | S'han implementat mesures de seguretat bàsiques a les oficines i despatxos, però cal millorar la gestió dels recursos físics. |
| **7.4** | Vigilància de la seguretat física | Sí | Implementat | Mitjà | S'han instal·lat càmeres de vigilància a punts clau, però es requereix una millor cobertura i supervisió del sistema. |
| **7.5** | Protecció contra les amenaces externes i ambientals | Sí | En implementació | Mitjà | Es requereixen mesures addicionals per protegir l'edifici i els recursos contra amenaces externes com incendis i inundacions. |
| **7.6** | El treball en àrees segures | Sí | Implementat | Alt | Les àrees segures s'han designat i s'apliquen normes estrictes per al seu accés i ús. |
| **7.7** | Política de lloc de treball clar i pantalla neta | Sí | En implementació | Mitjà | Cal establir polítiques més clares sobre l'ús de llocs de treball i la protecció de la informació. |
| **7.8** | Emplaçament i protecció d'equips | Sí | Implementat | Alt | Els equips estan ubicats en llocs segurs i protegits contra danys físics i accés no autoritzat. |
| **7.9** | Seguretat dels equips fora de les instal·lacions | Sí | En implementació | Mitjà | Es requereixen mesures addicionals per protegir els equips que estan fora de les instal·lacions de l'empresa. |
| **7.10** | Mitjans d'emmagatzematge | Sí | En implementació | Mitjà | S'han establert procediments per a l'emmagatzematge segur de la informació, però encara es requereix una millora en els sistemes de gestió. |
| **7.11** | Instal·lacions de subministrament | Sí | En implementació | Mitjà | Es requereixen mesures addicionals per garantir la seguretat de les instal·lacions de subministrament, com ara la protecció contra fallades elèctriques i sistemes de reserva. |
| **7.12** | Seguretat del cablejat | Sí | En implementació | Mitjà | Es requereix una millora en la gestió del cablejat per evitar danys físics i garantir la integritat de les connexions de xarxa. |
| **7.13** | Manteniment dels equips | Sí | Implementat | Alt | El manteniment regular dels equips s'ha dut a terme segons els procediments establerts per garantir el seu funcionament adequat. |
| **7.14** | Eliminació o reutilització segura d'equips | Sí | En implementació | Mitjà | Es requereixen polítiques i procediments per a la eliminació segura o la reutilització dels equips al final de la seva vida útil per evitar la pèrdua d'informació i protegir la seguretat. |
| **8** | **Tecnologia** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **8.1** | Dispositius de punt final d'usuari | Sí | Implementat | Mitjà | Els dispositius d'usuari estan configurats amb mesures bàsiques de seguretat, però la gestió i monitoratge de la seguretat és limitada. |
| **8.2** | Gestió de privilegis d'accés | Sí | Implementat | Mitjà | S'ha implementat una gestió bàsica de privilegis d'accés, però es requereix millorar la vigilància i revisió d'aquests privilegis. |
| **8.3** | Restricció d'accés a la informació | Sí | En implementació | Baix | S'estan començant a implementar mesures de restricció d'accés, però encara estan en les etapes inicials. |
| **8.4** | Accés al codi font dels programes | Sí | En implementació | Mitjà | Donat que no es desenvolupen programes internament, l'accés al codi font no és rellevant. |
| **8.5** | Autenticació segura | Sí | En implementació | Baix | S'estan explorant opcions per millorar l'autenticació, però encara no s'ha implementat cap solució significativa. |
| **8.6** | Gestió de capacitats | Sí | Implementat | Baix | Es fa una gestió bàsica de les capacitats dels sistemes, però no hi ha una optimització activa. |
| **8.7** | Controls contra el codi maliciós | Sí | En implementació | Mitjà | S'han implementat algunes eines bàsiques però no hi ha una defensa completa contra amenaces de codi maliciós. |
| **8.8** | Gestió de vulnerabilitats tècniques | Sí | En implementació | Baix | S'han identificat algunes vulnerabilitats, però encara no s'ha implementat un pla sistemàtic per gestionar-les. |
| **8.9** | Gestió de la configuració | Sí | Implementat | Baix | S'aplica una gestió de la configuració bàsica, però pot ser irregular i no sempre està documentada adequadament. |
| **8.10** | Eliminació de la informació | Sí | Implementat | Mitjà | S'elimina la informació obsoleta de manera ocasional, però no hi ha un procés establert i sistemàtic per fer-ho. |
| **8.11** | Emmascarament de dades | Sí | En implementació | Baix | Es duen a terme iniciatives per implementar l'emmascarament de dades, tot i que encara no s'ha completat la seva implementació. |
| **8.12** | Prevenció de fuites de dades | Sí | En implementació | Baix | S'estan explorant opcions per prevenir fuites de dades, però encara no s'ha implementat cap solució significativa. |
| **8.13** | Còpies de seguretat de la informació | Sí | Implementat | Baix | S'han realitzat còpies de seguretat de manera irregular, però no hi ha un pla de còpies de seguretat definit. |
| **8.14** | Redundància de les instal·lacions de processament d'informació | Sí | En implementació | Baix | S'estan considerant les mesures per introduir la redundància a les instal·lacions de processament d'informació, però encara no s'ha implementat cap solució concreta. |
| **8.15** | Registres | Sí | Implementat | Baix | Es mantenen registres d'activitats, però no sempre són exhaustius o fàcilment accessibles. |
| **8.16** | Seguiment d'activitats | Sí | En implementació | Baix | S'estan implementant eines de seguiment d'activitats, però encara no són àmpliament utilitzades o integrades en els processos. |
| **8.17** | Sincronització del rellotge | Sí | Implementat | Mitjà | Els rellotges dels diferents sistemes estan sincronitzats, però hi ha algunes discrepàncies ocasionals. |
| **8.18** | Ús de les utilitats amb privilegis del sistema | Sí | Implementat | Mitjà | Les utilitats amb privilegis del sistema s'utilitzen amb moderació i control, però hi ha àrees on s'ha de reforçar la supervisió. |
| **8.19** | Instal·lació del programari en entorn de producció | Sí | Implementat | Mitjà | El desplegament de programari en l'entorn de producció segueix un procés establert i ben documentat, assegurant la integritat i la disponibilitat dels serveis. |
| **8.20** | Controls de xarxa | Sí | Implementat | Mitjà | Es disposa de controls de xarxa per limitar l'accés no autoritzat als recursos de la xarxa interna i externa de la cooperativa Cal revisar i actualitzar el procediment conforme les exigències de la ISO 27001 |

| | | | | | |
|---|---|---|---|---|---|
| **8.21** | Seguretat dels serveis de xarxa | Sí | Implementat | Mitjà | Els serveis de xarxa estan configurats i gestionats de manera segura per protegir-los contra amenaces externes i internes. Cal revisar i actualitzar el procediment conforme les exigències de la ISO 27001 |
| **8.22** | Segregació en xarxes | Sí | Implementat | Mitjà | Les xarxes estan segregades per funció i nivell de sensibilitat de la informació, limitant l'exposició a possibles atacs. Cal revisar i actualitzarel procediment conforme les exigències de la ISO 27001 |
| **8.23** | Filtrat de webs | Sí | Implementat | Mitjà | Es disposa d'un filtre de webs per controlar i limitar l'accés a contingut web no desitjat o maliciós, però s'han detectat algunes limitacions en la seva eficàcia. Cal revisar i actualitzar el procediment conforme les exigències de la ISO 27001 |
| **8.24** | Ús de la criptografia | Sí | En implementació | Mitjà | Es plantegen línies de treball per implementar la criptografia en els diferents aspectes de la comunicació i l'emmagatzematge de la informació. |
| **8.25** | Seguretat en el cicle de vida dels desenvolupaments | Sí | En implementació | Baix | S'estan estudiant pràctiques per millorar la seguretat en totes les fases del cicle de vida dels desenvolupaments, però encara s'han de definir i implementar moltes mesures. |
| **8.26** | Requisits de seguretat de les aplicacions | Sí | En implementació | Baix | S'estan desenvolupant requisits de seguretat per a les aplicacions internes, però encara no s'han establert de manera sistemàtica. |
| **8.27** | Arquitectura segura de sistemes i principis d'enginyeria | Sí | En implementació | Mitjà | S'estan revisant els principis d'enginyeria de seguretat i s'està implementant una arquitectura més segura en els nous sistemes i actualitzant els existents. |
| **8.28** | Codificació segura | Sí | En implementació | Baix | Es duen a terme iniciatives de formació i s'estan estudiant pràctiques de codificació segura, però encara no s'han implementat de manera generalitzada. |
| **8.29** | Proves de seguretat en desenvolupament i acceptació | Sí | En implementació | Baix | Es realitzen algunes proves de seguretat durant el desenvolupament i la fase d'acceptació, però s'ha de millorar la seva cobertura i rigor. |
| **8.30** | Externalització del desenvolupament de programari | Sí | En implementació | Baix | S'està considerant l'externalització del desenvolupament de programari per a tasques específiques, però encara no s'ha dut a terme cap acció concreta en aquest sentit. |
| **8.31** | Separació dels recursos de desenvolupament, prova i operació | Sí | Implementat | Alt | S'han establert processos clars per separar els recursos de desenvolupament, prova i operació, evitant interferències i garantint la integritat dels sistemes. |
| **8.32** | Gestió de canvis | Sí | Implementat | Mitjà | Es disposa d'un procés de gestió de canvis per controlar les modificacions en els sistemes i garantir la seva integritat i disponibilitat, però encara s'han de realitzar millores en la seva implementació. |
| **8.33** | Dades de prova | Sí | En implementació | Baix | S'està treballant en l'establiment de dades de prova representatives per al desenvolupament i la prova, però encara no s'han definit completament. |
| **8.34** | Protecció dels sistemes d'informació durant l'auditoria i les proves | Sí | En implementació | Baix | Es duen a terme mesures per protegir els sistemes d'informació durant les auditories i les proves, però encara s'han de reforçar aquestes mesures per garantir la integritat i la confidencial |

Taula 50. Declaració d'Aplicabilitat

# Annex 4. Avaluació de la maduresa

| Sec. | Mesura ISO 27001:2023 | M. inicial | M. final | CMM | Justificació |
|---|---|---|---|---|---|
| **4** | **Context de l'organització** | **1,75** | **3,75** | **L3** | |
| 4,1 | Context organitzacional | 2 | 4 | L4 | S'ha establert un procés sistemàtic per revisar i entendre el context organitzacional, assegurant que els objectius del SGSI estan alineats amb els objectius estratègics de la cooperativa. |
| 4,1 | Determinar els objectius de l'SGSI de l'organització i qualsevol qüestió que en pugui comprometre l'efectivitat | 2 | 4 | L4 | S'han definit i documentat clarament els objectius del SGSI, i s'han establert mecanismes per avaluar i mitigar qualsevol qüestió que pugui comprometre la seva efectivitat. |
| 4,2 | Comprensió partes interessades | 3 | 4 | L4 | S'ha ampliat la identificació de parts interessades i s'ha assegurat que totes les obligacions legals i normatives estan clarament documentades i complertes. |
| 4.2 (a) | Identificar les parts interessades incloent-hi lleis aplicables, regulacions, contractes, etc. | 3 | 4 | L4 | S'han identificat exhaustivament totes les parts interessades i s'ha assegurat el compliment de totes les lleis i regulacions rellevants. |
| 4.2 (b) | Determinar els requisits rellevants respecte a la seguretat de la informació i les obligacions. | 3 | 4 | L4 | S'han establert processos per identificar i documentar tots els requisits rellevants, assegurant la seva implementació efectiva. |
| 4,3 | Abast del SGSI | 1 | 3 | L3 | S'ha definit i documentat clarament l'abast del SGSI, assegurant que inclou tots els aspectes crítics de l'organització. |
| 4,3 | Determinar y documentar l'abast del SGSI | 1 | 3 | L3 | S'ha completat la documentació de l'abast del SGSI, incloent tots els processos i actius rellevants. |
| 4,4 | SGSI | 1 | 4 | L4 | S'ha establert, implementat i mantingut un SGSI completament funcional que segueix les directrius de la norma ISO/IEC 27001. |
| 4,4 | Establir, implementar, mantenir i millorar contínuament un SGSI de conformitat amb la norma | 1 | 4 | L4 | S'ha implementat un procés de millora contínua per assegurar que el SGSI es manté actualitzat i efectiu. |
| **5** | **Lideratge** | **1,66** | **3,67** | **L3** | |
| 5,1 | Lideratge i compromís | 2 | 3 | L3 | La direcció ha augmentat el seu lideratge visible i ha participat activament en la implementació del SGSI. |
| 5,1 | La alta direcció ha de demostrar lideratge & compromís en relació con el SGSI. | 2 | 3 | L3 | La direcció ha mostrat un lideratge més actiu i ha proporcionat recursos i suport per a la implementació del SGSI. |
| 5,2 | Política | 1 | 4 | L3 | S'ha establert i comunicat una política de seguretat de la informació que ha estat aprovada per la direcció. |
| 5,2 | Establir la política de seguretat de la informació | 1 | 4 | L3 | La política de seguretat de la informació ha estat formalment establerta i està alineada amb els objectius estratègics de |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | l'organització. |
| 5,3 | Rols, responsabilitats i autoritats en la organització | 2 | 4 | L4 | S'han assignat i comunicat clarament els rols i responsabilitats en matèria de seguretat de la informació a tots els nivells de l'organització. |
| 5,3 | Assignar y comunicar els rols i les responsabilitats de la seguretat de la informació. | 2 | 4 | L4 | Tots els empleats han estat informats dels seus rols i responsabilitats, i s'han establert equips específics per gestionar la seguretat de la informació. |
| **6** | **Planificació** | **1,77** | **3,87** | **L3** | |
| 6,1 | Accions per tractar amb els riscos i oportunitats | 1,33 | 3,66 | L3 | S'han identificat i planificat accions específiques per tractar amb els riscos i oportunitats relacionats amb la seguretat de la informació. |
| 6.1.1 | Dissenyar / planificar el SGSI per satisfer els requisits, tractant amb els riscos & oportunitats | 2 | 4 | L3 | S'ha dissenyat un SGSI complet que aborda tots els requisits, riscos i oportunitats de manera efectiva. |
| 6.1.2 | Definir i aplicar un procés d'apreciació de riscs de seguretat de la informació. Documentar i aplicar un procés de tractament de riscos de seguretat de la informació | 1 | 3 | L3 | S'han definit i aplicat processos per a l'apreciació i tractament dels riscos de seguretat de la informació, assegurant que es documentin adequadament. |
| 6.1.3 | Documentar i aplicar un procés de tractament de riscos de seguretat de la informació | 1 | 4 | L3 | S'ha documentat i aplicat un procés exhaustiu de tractament de riscos que garanteix la gestió efectiva dels riscos identificats. |
| 6,2 | Objectius i plans de seguretat de la informació | 2 | 4 | L4 | S'han establert objectius clars i plans detallats per a la seguretat de la informació, assegurant la seva implementació i seguiment. |
| 6,2 | Establir i documentar els objectius i els plans de seguretat de la informació | 2 | 4 | L3 | Els objectius i plans de seguretat de la informació han estat documentats i alineats amb les estratègies de l'organització. |
| 6,3 | Planificació de canvis | 2 | 4 | L4 | S'ha establert un procés formal per planificar i gestionar els canvis substancials al SGSI de manera controlada. |
| 6,3 | Els canvis substancials a l'SGSI s'han de dur a terme de manera planificada | 2 | 4 | L4 | Els canvis substancials es planifiquen i implementen de manera estructurada, assegurant la seva efectivitat i coherència amb el SGSI. |
| **7** | **Suport** | **2,26** | **3,6** | **L3** | |
| 7,1 | Recursos | 2 | 4 | L4 | S'han determinat i proporcionat tots els recursos necessaris per a la implementació i manteniment efectiu del SGSI. |
| 7,1 | Determinar i proporcionar els recursos necessaris per al SGSI | 2 | 4 | L4 | La cooperativa ha assegurat la disponibilitat dels recursos necessaris per mantenir el SGSI operatiu i efectiu. |
| 7,2 | Competències | 3 | 4 | L4 | S'han determinat i documentat les competències necessàries, i s'ha garantit la formació adequada de tot el personal. |
| 7,2 | Determinar, documentar i | 3 | 4 | L4 | Les competències necessàries per a la |

| | | | | | |
|---|---|---|---|---|---|
| | posar a disposició les competències necessàries | | | | gestió de la seguretat de la informació s'han determinat, documentat i proporcionat de manera efectiva. |
| 7,3 | Conscienciació | 3 | 4 | L4 | S'ha establert un programa de conscienciació continuat que ha augmentat la comprensió i importància de la seguretat de la informació entre tot el personal. |
| 7,3 | Establir un programa de conscienciació en seguretat | 3 | 4 | L4 | S'han dut a terme programes de conscienciació regulars que han millorat significativament la cultura de seguretat de la informació dins de l'organització. |
| 7,4 | Comunicació | 2 | 3 | L3 | S'han establert procediments per a la comunicació interna i externa rellevant al SGSI, assegurant una transmissió efectiva de la informació. |
| 7,4 | Determinar la necessitat per a les comunicacions internes i externes rellevants a l'SGSI | 2 | 3 | L3 | S'han determinat les necessitats de comunicació i s'han establert protocols per assegurar que tota la informació rellevant sigui comunicada de manera efectiva. |
| 7,5 | Informació documentada | 1,33 | 3 | L3 | S'ha millorat la gestió de la documentació, assegurant que tota la informació requerida sigui adequada, controlada i accessible. |
| 7.5.1 | Proveir la documentació requerida per la norma així com la requerida per l'organització | 2 | 3 | L3 | S'ha assegurat que tota la documentació requerida per la norma i l'organització està disponible i actualitzada. |
| 7.5.2 | Proveir títols, autors, etc per a la documentació, adequar el format. | 1 | 3 | L3 | S'han establert estàndards per a la documentació, assegurant que tot el material sigui clarament titulat, autoritzat i formatat adequadament. |
| 7.5.3 | Controlar la documentació adequadament | 1 | 3 | L3 | S'han implementat controls efectius per gestionar la documentació, assegurant la seva integritat i disponibilitat. |
| **8** | **Operació** | **1** | **3,67** | **L3** | |
| 8,1 | Planificació i control operacional | 1 | 3 | L3 | S'han establert plans i controls operacionals per gestionar els riscos de seguretat de la informació de manera efectiva. |
| 8,1 | Planificar, implementar, controlar i documentar el procés de l'SGSI per gestionar els riscos (ex. un pla de tractament de riscos) | 1 | 3 | L3 | S'ha planificat, implementat i documentat el procés del SGSI per gestionar els riscos, incloent-hi un pla de tractament de riscos. |
| 8,2 | Apreciació del risc de seguretat de la informació | 1 | 4 | L4 | S'ha establert un procés regular per a l'apreciació i documentació dels riscos de seguretat de la informació, assegurant una revisió constant. |
| 8,2 | (Re)fer l'apreciació i documentar els riscos de seguretat de la informació en forma regular & davant de canvis o modificacions | 1 | 4 | L4 | S'ha implementat un procés per reavaluar i documentar regularment els riscos de seguretat de la informació, especialment davant de canvis. |
| 8,3 | Tractament del risc de seguretat de la informació | 1 | 4 | L4 | S'ha implementat i documentat un pla de tractament de riscos, assegurant que totes les accions correctives es duguin a terme de manera efectiva. |

| | | | | | |
|---|---|---|---|---|---|
| 8,3 | Implementar el pla de tractament de riscos i documentar-ne els resultats | 1 | 4 | L4 | S'ha assegurat la implementació i documentació dels resultats del pla de tractament de riscos, millorant la gestió de riscos. |
| **9** | **Avaluació de l'exercici** | **1** | **4** | **L4** | |
| 9,1 | Seguiment, mesura, anàlisi i avaluació | 1 | 4 | L4 | S'han establert processos per al seguiment, mesura, anàlisi i avaluació del SGSI i els seus controls, assegurant la seva efectivitat contínua. |
| 9,1 | Fer seguiment, mesurar, analitzar i avaluar l'SGSI i els controls | 1 | 4 | L4 | S'ha millorat el procés de seguiment, mesura, anàlisi i avaluació per assegurar una gestió efectiva del SGSI. |
| 9,2 | Auditoria interna | 1 | 4 | L4 | S'han planificat i dut a terme auditories internes regulars del SGSI per identificar àrees de millora i assegurar el compliment dels requisits. |
| 9,2 | Planificar i dur a terme auditories internes de l'SGSI | 1 | 4 | L4 | Les auditories internes s'han realitzat de manera regular, assegurant que el SGSI sigui avaluat i millorat contínuament. |
| 9,3 | Revisió per la direcció | 1 | 4 | L4 | La direcció ha realitzat revisions periòdiques del SGSI per assegurar la seva alineació amb els objectius estratègics i identificar àrees de millora. |
| 9,3 | Emprendre revisions per la direcció del SGSI regularment | 1 | 4 | L4 | Les revisions regulars per part de la direcció han assegurat que el SGSI es manté efectiu i alineat amb les necessitats de l'organització. |
| **10** | **Millora** | **1** | **3,5** | **L3** | |
| 10,1 | Millora continua | 1 | 4 | L4 | S'ha implementat un procés de millora contínua per assegurar que el SGSI s'adapta i evoluciona amb les necessitats canviants de l'organització. |
| 10,1 | Millorar contínuament el SGSI | 1 | 4 | L4 | S'han establert mecanismes per a la millora contínua, assegurant que el SGSI es manté efectiu i en constant evolució. |
| 10,2 | No conformitat i accions correctives | 1 | 3 | L3 | S'han implementat processos per identificar, corregir i prevenir la recurrència de no-conformitats, documentant totes les accions correctives preses. |
| 10,2 | Identificar, corregir i dur a terme accions per prevenir la recurrència de no-conformitats, documentant les accions | 1 | 3 | L3 | S'han millorat els processos per gestionar no-conformitats, assegurant que es documentin i es previnguin de manera efectiva. |

Taula 51. Valoració de la maduresa assolida en la ISO 27001:2023

| Sec. | Controls ISO 27002:2023 | M. inicial | M. final | CMM | Justificació |
|---|---|---|---|---|---|
| 5 | Organització | 1,756 | 3,46 | L3 | |
| 5.1 | Polítiques de seguretat de la informació | 2 | 4 | L4 | Les polítiques s'han documentat, comunicat, i ara es mesuren amb indicadors numèrics per garantir la seva efectivitat. |
| 5.2 | Rols i responsabilitats en seguretat de la informació | 2 | 4 | L4 | Els rols i responsabilitats estan clarament definits, documentats i comunicats, amb eines de mesura per fer-ne seguiment. |
| 5.3 | Segregació de tasques | 3 | 4 | L4 | La segregació de tasques està implantada i mesurada, amb eines que garanteixen la qualitat i eficiència del procés. |
| 5.4 | Responsabilitats de la direcció | 1 | 3 | L3 | La direcció ara participa activament en la supervisió, amb processos definits i comunicats a través d'entrenament formal. |
| 5.5 | Contacte amb les autoritats | 1 | 3 | L3 | Establerts protocols documentats i entrenament formal per contactar amb autoritats en cas d'incidents de seguretat. |
| 5.6 | Contacte amb grups d'informació especials | 1 | 3 | L3 | Participació formal en grups d'informació amb processos documentats i comunicats. |
| 5.7 | Intel·ligència d'amenaces | 1 | 3 | L3 | Implementats processos per recopilar i analitzar intel·ligència d'amenaces amb documentació i entrenament formal. |
| 5.8 | Seguretat de la informació en la gestió de projectes | 1 | 4 | L4 | Integració formal de la seguretat en la gestió de projectes amb indicadors per mesurar-ne l'eficàcia. |
| 5.9 | Inventari d'informació i altres actius associats | 3 | 4 | L4 | Inventari complet amb controls de seguretat mesurats per garantir la seva actualització constant. |
| 5.10 | Ús acceptable de la informació i actius associats | 2 | 3 | L3 | Polítiques d'ús acceptable definides, documentades i comunicades amb entrenament formal. |
| 5.11 | Devolució d'actius | 1 | 3 | L3 | Procediments establerts i documentats per a la devolució d'actius, amb entrenament formal per al personal. |
| 5.12 | Classificació de la informació | 3 | 4 | L4 | Sistemes de classificació de la informació documentats i mesurats per garantir la seva aplicació correcta. |
| 5.13 | Etiquetatge de la informació | 1 | 3 | L3 | Procediments documentats i entrenament formal per a l'etiquetatge de la informació. |
| 5.14 | Transferència de la informació | 2 | 3 | L3 | Definits i documentats processos per a la transferència segura de la informació, amb entrenament formal. |
| 5.15 | Control d'accés | 3 | 4 | L4 | Controls d'accés definits, documentats i mesurats amb eines per assegurar la seva eficàcia. |
| 5.16 | Gestió d'identitat | 3 | 4 | L4 | Processos de gestió d'identitat implantats, documentats i mesurats amb eines tecnològiques. |

| | | | | | |
|---|---|---|---|---|---|
| 5.17 | Informació d'autenticació | 2 | 3 | L3 | Processos d'autenticació definits, documentats i entrenament formal per assegurar-ne el compliment. |
| 5.18 | Drets d'accés | 2 | 4 | L4 | Drets d'accés clarament definits, documentats i mesurats amb eines per garantir el control adequat. |
| 5.19 | Seguretat de la informació en les relacions amb els proveïdors | 3 | 4 | L4 | Processos de seguretat amb proveïdors documentats i mesurats per garantir el compliment dels acords. |
| 5.20 | Abordar la seguretat de la informació dins dels acords de proveïdors | 2 | 3 | L3 | Acords de seguretat documentats i comunicats formalment amb els proveïdors. |
| 5.21 | Gestió de la seguretat de la informació a la cadena de subministrament de les TIC | 1 | 3 | L3 | Processos documentats i entrenament formal per gestionar la seguretat a la cadena de subministrament de TIC. |
| 5.22 | Seguiment, revisió i gestió del canvi dels serveis de proveïdors | 3 | 4 | L4 | Processos de seguiment i revisió definits, documentats i mesurats per assegurar la gestió del canvi amb els proveïdors. |
| 5.23 | Seguretat de la informació per a l'ús de serveis al núvol | 1 | 3 | L3 | Implementació de protocols de seguretat per a l'ús de serveis al núvol, amb documentació i entrenament formal. |
| 5.24 | Planificació i preparació de la gestió d'incidents de seguretat d'informació | 2 | 3 | L3 | Plans documentats i comunicats per gestionar incidents de seguretat, amb entrenament formal per al personal. |
| 5.25 | Avaluació i decisió sobre els esdeveniments de seguretat d'informació | 1 | 3 | L3 | Processos establerts, documentats i entrenament formal per avaluar i decidir sobre esdeveniments de seguretat. |
| 5.26 | Resposta a incidents de seguretat de la informació | 1 | 3 | L3 | Procediments documentats i entrenament formal per respondre a incidents de seguretat de la informació. |
| 5.27 | Aprenentatge dels incidents de seguretat de la informació | 1 | 3 | L3 | Processos documentats per analitzar i aprendre dels incidents de seguretat, amb entrenament formal. |
| 5.28 | Recull d'evidències | 1 | 3 | L3 | Procediments establerts i documentats per a la recollida d'evidències, amb entrenament formal per al personal. |
| 5.29 | Seguretat de la informació durant la interrupció | 1 | 3 | L3 | Plans documentats i entrenament formal per assegurar la seguretat de la informació durant interrupcions. |
| 5.30 | Preparació per a les TIC per a la continuïtat del negoci | 1 | 4 | L4 | Processos de continuïtat del negoci documentats, mesurats i amb eines tecnològiques per garantir la seva efectivitat. |
| 5.31 | Identificació de requisits legals, reglamentaris i contractuals | 3 | 4 | L4 | Requisits identificats, documentats i mesurats per assegurar el compliment legal i reglamentari. |
| 5.32 | Drets de propietat intel·lectual (DPI) | 2 | 3 | L3 | Processos documentats per gestionar els DPI, amb entrenament formal per al personal. |
| 5.33 | Protecció dels registres de l'organització | 2 | 4 | L4 | Sistemes de protecció dels registres documentats i mesurats per garantir la seva seguretat. |

| | | | | | |
|---|---|---|---|---|---|
| 5.34 | Privadesa i protecció de la informació d'identificació personal | 2 | 4 | L4 | Polítiques de privadesa documentades, comunicades i mesurades per garantir la protecció de la informació personal. |
| 5.35 | Revisió independent de la seguretat de la informació | 1 | 3 | L3 | Procediments documentats per a revisions independents de seguretat, amb entrenament formal per als revisors. |
| 5.36 | Compliment de les polítiques i normes de seguretat de la informació | 2 | 4 | L4 | Polítiques i normes complides, documentades i mesurades amb indicadors per garantir l'eficàcia. |
| 5.37 | Documentació de procediments d'operació | 1 | 4 | L4 | Procediments d'operació documentats i mesurats amb eines per assegurar-ne la qualitat i eficiència. |
| **6** | **Persones** | **2,5** | **3,75** | **L3** | |
| 6.1 | Comprovació | 2 | 3 | L3 | Procediments establerts i documentats per a la comprovació de seguretat, amb entrenament formal. |
| 6.2 | Termes i condicions de contractació | 3 | 4 | L4 | Termes i condicions documentats i mesurats per assegurar el seu compliment. |
| 6.3 | Conscienciació, educació i formació en seguretat de la informació | 2 | 4 | L4 | Programes de formació i conscienciació documentats, comunicats i mesurats per garantir la seva efectivitat. |
| 6.4 | Procés disciplinari | 2 | 3 | L3 | Processos disciplinaris establerts, documentats i comunicats amb entrenament formal. |
| 6.5 | Responsabilitat davant la finalització o canvi | 3 | 4 | L4 | Responsabilitats clarament definides, documentades i mesurades per assegurar la seva aplicació. |
| 6.6 | Acords de confidencialitat o no divulgació | 3 | 4 | L4 | Acords documentats i mesurats per garantir la confidencialitat i no divulgació de la informació. |
| 6.7 | Treball en remot | 3 | 4 | L4 | Procediments de seguretat per al treball remot documentats i mesurats per assegurar-ne l'eficàcia. |
| 6.8 | Notificació dels esdeveniments de seguretat de la informació | 2 | 4 | L4 | Sistemes de notificació documentats, comunicats i mesurats per garantir una resposta ràpida i eficient. |
| **7** | **Infraestructura** | **2,214** | **3,64** | **L3** | |
| 7.1 | Perímetre de seguretat física | 3 | 4 | L4 | Perímetres de seguretat definits, documentats i mesurats per garantir la seva protecció. |
| 7.2 | Controls físics d'entrada | 3 | 4 | L4 | Controls d'entrada documentats i mesurats amb eines per assegurar-ne l'eficàcia. |
| 7.3 | Seguretat d'oficines, despatxos i recursos | 3 | 4 | L4 | Procediments de seguretat per a oficines i recursos documentats i mesurats per garantir la seva protecció. |
| 7.4 | Vigilància de la seguretat física | 3 | 4 | L4 | Sistemes de vigilància documentats i mesurats per assegurar la seva efectivitat. |
| 7.5 | Protecció contra les amenaces externes i ambientals | 1 | 3 | L3 | Processos documentats per a la protecció contra amenaces externes, amb entrenament formal per al personal. |

| | | | | | |
|---|---|---|---|---|---|
| 7.6 | El treball en àrees segures | 3 | 4 | L4 | Àrees segures documentades i mesurades per garantir la seva protecció. |
| 7.7 | Política de lloc de treball clar i pantalla neta | 2 | 3 | L3 | Polítiques documentades i comunicades per assegurar el compliment del lloc de treball clar i pantalla neta. |
| 7.8 | Emplaçament i protecció d'equips | 2 | 3 | L3 | Processos documentats per a l'emplaçament i protecció d'equips, amb entrenament formal per al personal. |
| 7.9 | Seguretat dels equips fora de les instal·lacions | 2 | 3 | L3 | Procediments establerts i documentats per a la seguretat d'equips fora de les instal·lacions, amb entrenament formal. |
| 7.10 | Mitjans d'emmagatzematge | 2 | 4 | L4 | Sistemes d'emmagatzematge documentats i mesurats per garantir la seva seguretat. |
| 7.11 | Instal·lacions de subministrament | 3 | 4 | L4 | Processos de seguretat per a instal·lacions de subministrament documentats i mesurats per assegurar-ne l'eficàcia. |
| 7.12 | Seguretat del cablejat | 1 | 4 | L4 | Sistemes de seguretat del cablejat documentats i mesurats per garantir la seva protecció. |
| 7.13 | Manteniment dels equips | 2 | 4 | L4 | Procediments de manteniment documentats i mesurats per assegurar la seva eficàcia. |
| 7.14 | Eliminació o reutilització segura d'equips | 1 | 3 | L3 | Processos establerts i documentats per a l'eliminació o reutilització segura d'equips, amb entrenament formal. |
| **8** | **Tecnologia** | **2,029** | **3,68** | **L3** | |
| 8.1 | Dispositius de punt final d'usuari | 1 | 3 | L3 | Procediments documentats per a la gestió de dispositius de punt final, amb entrenament formal. |
| 8.2 | Gestió de privilegis d'accés | 3 | 4 | L4 | Privilegis d'accés definits, documentats i mesurats per assegurar el control adequat. |
| 8.3 | Restricció d'accés a la informació | 2 | 3 | L3 | Processos de restricció d'accés documentats i comunicats amb entrenament formal per assegurar el compliment. |
| 8.4 | Accés al codi font dels programes | 2 | 3 | L3 | Procediments documentats per a l'accés al codi font, amb entrenament formal per assegurar-ne la seguretat. |
| 8.5 | Autenticació segura | 2 | 3 | L3 | Sistemes d'autenticació documentats i comunicats amb entrenament formal per garantir la seva seguretat. |
| 8.6 | Gestió de capacitats | 1 | 3 | L3 | Processos documentats per a la gestió de capacitats, amb entrenament formal per al personal. |
| 8.7 | Controls contra el codi maliciós | 2 | 4 | L4 | Sistemes de control contra codi maliciós documentats i mesurats per assegurar la seva efectivitat. |
| 8.8 | Gestió de vulnerabilitats tècniques | 2 | 4 | L4 | Processos de gestió de vulnerabilitats documentats i mesurats amb eines per assegurar la seva efectivitat. |
| 8.9 | Gestió de la configuració | 3 | 4 | L4 | Procediments de gestió de la configuració documentats i mesurats |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | per garantir la seva eficàcia. |
| 8.10 | Eliminació de la informació | 2 | 3 | L3 | Processos documentats per a l'eliminació segura de la informació, amb entrenament formal per al personal. |
| 8.11 | Emmascarament de dades | 1 | 3 | L3 | Sistemes d'emmascarament de dades documentats i comunicats amb entrenament formal. |
| 8.12 | Prevenció de fuites de dades | 2 | 4 | L4 | Sistemes de prevenció de fuites documentats i mesurats per garantir la seva efectivitat. |
| 8.13 | Còpies de seguretat de la informació | 2 | 4 | L4 | Processos de còpies de seguretat documentats i mesurats per assegurar la seva eficàcia. |
| 8.14 | Redundància de les instal·lacions de processament d'informació | 2 | 4 | L4 | Sistemes de redundància documentats i mesurats per garantir la continuïtat del processament d'informació. |
| 8.15 | Registres | 2 | 4 | L4 | Processos de gestió de registres documentats i mesurats per assegurar la seva seguretat. |
| 8.16 | Seguiment d'activitats | 3 | 4 | L4 | Sistemes de seguiment documentats i mesurats per garantir la seva eficàcia. |
| 8.17 | Sincronització del rellotge | 3 | 4 | L4 | Sistemes de sincronització del temps documentats i mesurats per assegurar la seva precisió. |
| 8.18 | Ús de les utilitats amb privilegis del sistema | 3 | 4 | L4 | Sistemes de seguretat de comunicacions documentats i mesurats per garantir la seva protecció. |
| 8.19 | Instal·lació del programari en entorn de producció | 3 | 4 | L4 | Procediments de seguretat de la xarxa documentats i mesurats per assegurar la seva eficàcia. |
| 8.20 | Controls de xarxa | 3 | 4 | L4 | Processos de seguretat per als serveis de xarxa documentats i mesurats per garantir la seva protecció. |
| 8.21 | Seguretat dels serveis de xarxa | 3 | 4 | L4 | Procediments documentats per a la transferència segura de la informació, amb entrenament formal per al personal. |
| 8.22 | Segregació en xarxes | 3 | 4 | L4 | Acords de telecomunicacions documentats i mesurats per assegurar la seva confidencialitat. |
| 8.23 | Filtrat de webs | 0 | 3 | L3 | Requisits de seguretat documentats i comunicats amb entrenament formal per assegurar el seu compliment. |
| 8.24 | Ús de la criptografia | 2 | 4 | L4 | Processos documentats per al processament de dades sensibles, amb entrenament formal per assegurar-ne la seguretat. |
| 8.25 | Seguretat en el cicle de vida dels desenvolupaments | 1 | 4 | L4 | Procediments documentats per a la gestió de servidors d'aplicació, amb entrenament formal per assegurar la seva seguretat. |
| 8.26 | Requisits de seguretat de les aplicacions | 1 | 4 | L4 | Processos establerts i documentats per al desenvolupament de sistemes d'informació, amb entrenament formal. |

| | | | | | |
|---|---|---|---|---|---|
| 8.27 | Arquitectura segura de sistemes i principis d'enginyeria | 2 | 4 | L4 | Sistemes de desenvolupament segur documentats i comunicats amb entrenament formal per assegurar la seva aplicació. |
| 8.28 | Codificació segura | 1 | 4 | L4 | Procediments establerts i documentats per a la seguretat en entorns de desenvolupament i prova, amb entrenament formal. |
| 8.29 | Proves de seguretat en desenvolupament i acceptació | 3 | 4 | L4 | Processos documentats per a la gestió de programari de sistemes d'informació, amb entrenament formal per al personal. |
| 8.30 | Externalització del desenvolupament de programari | 3 | 4 | L4 | Procediments establerts i documentats per a la seguretat del codi font, amb entrenament formal per assegurar la seva protecció. |
| 8.31 | Separació dels recursos de desenvolupament, prova i operació | 3 | 4 | L4 | Processos documentats per a la gestió de IA i ML, amb entrenament formal per assegurar la seva aplicació segura. |
| 8.32 | Gestió de canvis | 1 | 3 | L3 | Sistemes de protecció de serveis de registre i directoris documentats i mesurats per assegurar la seva seguretat. |
| 8.33 | Dades de prova | 1 | 3 | L3 | Sistemes de monitoratge documentats i mesurats per garantir la seguretat en aplicacions. |
| 8.34 | Protecció dels sistemes d'informació durant l'auditoria i les proves | 1 | 3 | L3 | Requisits de seguretat per a serveis en núvol documentats i mesurats per garantir la seva protecció. |

Taula 52. Valoració de la maduresa assolida en els controls ISO 27002:2023