Sistemes de gestió de la seguretat de la informació

Nom Estudiant: Margalida Pau Canet Urrea

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

Consultor: José Luis Dürsteler Esteban
Professor responsable de l'assignatura: Carles Garrigues Olivella
Centre: Universitat Oberta de Catalunya
Data Lliurament: Juny 2022

FITXA DEL TREBALL FINAL

Títol del treball:	*Sistemes de gestió de seguretat de la informació*
Nom de l'autor:	*Margalida Pau Canet Urrea*
Nom del consultor/a:	*José Luis Dürsteler Esteban*
Nom del PRA:	*Carles Garrigues Olivella*
Data de lliurament (mm/aaaa):	*06/2022*
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	*SGSI, PDS, Auditoria*

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

El Treball de Final de Màster està contextualitzat en l'àrea de Sistemes de Gestió de Seguretat de la Informació, el qual consisteix precisament a implementar un Sistema de Gestió de Seguretat de la Informació (SGSI) a una organització que basa la seva activitat de negoci amb la gestió hotelera, basant-nos en la norma ISO/IEC 27001:2013 i el seu annex, ISO/IEC 27002. En concret, hem definit l'abast del Pla Director de Seguretat (PDS) en l'oficina central de la divisió hotelera seleccionada, on es vol protegir els següents processos de negoci: procés de venda, la informació dels clients, la informació confidencial de l'empresa i el software de la gestió hotelera.

El treball està orientat a establir les bases del PDS implementat per un SGSI des del seu inici, realitzant una anàlisi de la situació actual, definir la política de seguretat de l'empresa, revisar la gestió de rols i responsabilitats, elaborar una anàlisi de riscos juntament amb la declaració d'aplicabilitat, realitzar un inventari d'actius de l'organització, analitzar les possibles amenaces i el seu impacte i probabilitat, descriure propostes de projectes de millora i finalment amb tota aquesta informació, realitzar l'auditoria de compliment de la ISO/IEC 27001:2013.

Un cop finalitzat el treball i haver duit a terme l'execució d'aquest projecte, podem dir que s'han millorat certs aspectes de la Seguretat de la Informació de l'organització, tot i que no s'ha arribat al nivell desitjat que s'havia proposat podem dir que s'han assolit els objectius d'aquest PDS.

Abstract (in English, 250 words or less):

The Master's Thesis is contextualised in Information Security Management Systems, which consists precisely in implementing an Information Security Management System (ISMS) in an organisation that bases its business activity with hotel management, based on ISO / IEC 27001: 2013 and its annexe, ISO / IEC 27002. Specifically, we have defined the scope of the Security Master Plan (PDS) in the central office of the selected hotel division, where you want to protect the following business processes: sales process, customer information, confidential company information and hotel management software.

The work is aimed at establishing the basis of the PDS implemented by an ISMS since its inception, conducting a first analysis of the current situation, defining the company's security policy, reviewing the management of roles and responsibilities, and developing an analysis of risks together with the declaration of applicability, make an inventory of the organisation's assets, analyse possible threats and their impact and probability, describe proposals for improvement projects and finally with all this information, perform the compliance audit of ISO / IEC 27001: 2013.

Once has been completed and this project has been carried out, we can say that certain aspects of the organization's Information Security have been improved. Although the desired level has not been reached, we can say that this PDS has been successfully completed.

Índex

Llista de figures

Llista de taules

1. Introducció

1.1 Context i justificació del Treball

La tecnologia de la informació i comunicació ha sofert una gran evolució aquesta darrera dècada, la qual cosa ens ha permès automatitzar i optimitzar la majoria de les activitats que es duen a terme a la nostra organització. A poc a poc aquestes tecnologies han anat ocupant més àrees de l'empresa fins al punt que avui en dia no podem dur a terme segons quines activitats sense l'ús d'aquestes. Aleshores podem afirmar que les empreses basen la seva activitat de negoci en sistemes de la informació suportats per dispositius tecnològics.

Per això és molt important protegir els sistemes d'informació de la nostra empresa amb la gestió de les actuacions en matèria de ciberseguretat, independentment de les dimensions d'aquesta. Per tal de poder dur a terme les activitats de manera satisfactòria per l'empresa, redactarem el Pla Director de Seguretat (PDS).

El Pla Director de Seguretat consisteix en definir i prioritzar un conjunt de projectes relacionats en la seguretat de la informació per tal de minimitzar els riscs als quals està exposada l'organització fins a aconseguir uns nivells acceptables d'aquests, a partir d'una anàlisi de la situació inicial.

Per tal de fer front a aquest projecte caldrà establir les bases del Pla Director de Seguretat, on analitzarem l'inventari d'actius de l'empresa, estudiarem les amenaces a les quals esteim exposats, estudiarem l'impacte potencial d'aquestes, proposarem un pla d'acció per a lluitar contra aquestes amenaces i un cop aplicat el pla d'acció, avaluarem l'impacte residual d'aquest.

1.2 Objectius del Treball

L'objectiu principal de la realització d'aquest Treball de Fi de Màster (TFM) és analitzar els sistemes de la informació de l'empresa seleccionada i implantar un Sistema de Gestió de la Informació (SGSI) segons la normativa vigent, els estàndards internacionals com la ISO27001 i la Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes d'Informació (MAGERIT). És a dir, l'objectiu és establir per als sistemes d'informació actuals de l'empresa una metodologia de treball que permeti la seva gestió, acord amb els objectius de creixement de l'empresa. On també serà necessari el desenvolupament d'un pla per assegurar la disponibilitat dels serveis garantint el correcte funcionament dels processos del propi negoci. Aquest objectiu principal es pot desenvolupar en tres subobjectius que són els següents:

- Avaluació de la situació actual i l'entorn per identificar els riscs sobre la seguretat de la informació.
- Identificació de les àrees de l'empresa que estan més exposades al risc, en funció de la gravetat de l'impacte i de la probabilitat que això succeeixi.

- Adoptar les mesures necessàries per reduir al mínim possible aquests riscs.

A més d'aquests objectius tècnics, és important destacar altres objectius com per exemple aportar major confiança als clients mitjançant l'obtenció del pla director de seguretat, ja que així les seves dades estan més protegides.

Quan s'aconsegueixin tots aquests objectius l'empresa aconseguirà una sèrie d'avantatges com per exemple una major eficàcia en el departament d'IT i alhora s'aconseguirà un avantatge competitiu amb la resta d'empreses competidores.

Cal tenir en compte que els propòsits s'hauran d'anar revisant temporalment i adaptant a les necessitats de l'empresa, ja que es tracta d'un procés de millora continua PDCA (Plan-Do-Check-Act). D'aquesta manera en cada actualització es podran avaluar els progressos tecnològics de l'empresa segons les tendències tecnològiques del mercat.

1.3 Enfocament i mètode seguit

A l'hora de desenvolupar un projecte com aquest ens plantejam diverses possibles estratègies, la primera de totes, si hem de crear un nou PDS o bé realitzam una actualització d'un PDS ja existent. I llavors, si contractam els serveis de consultoria per a l'elaboració del projecte o si ho realitzam internament.

L'estratègia seleccionada consisteix en desenvolupar un producte nou, que consisteix en la creació d'un Pla Director de Seguretat. L'elecció d'aquesta estratègia ha estat perquè l'empresa seleccionada no disposa actualment d'un Pla Director de Seguretat. En cas de tenir-ne un, la tasca hauria estat fer-ne la revisió, però com que no és així, el crearem.

La metodologia per desenvolupar el Pla Director de Seguretat consisteix en una sèrie de fases consecutives seguint els objectius prèviament fitxats. És molt important realitzar cada una d'aquestes activitats de manera estricta segons els objectius que hem definit. En el nostre cas, realitzarem el procés en sis etapes, que són les següents:

- Fase 1 – Contextualització i documentació.

Introducció al projecte. Enfocament i selecció de l'empresa que serà objecte d'estudi. Definició dels objectius del Pla Director de Seguretat i Anàlisi diferencial de l'empresa respecte a la ISO/IEC 27001 i ISO/IEC 27002.

- Fase 2 – Sistema de gestió documental.

Elaboració de la Política de Seguretat. Declaració de l'aplicabilitat i documentació del SGSI.

- Fase 3 – Estat del risc: identificació i valoració.

Elaboració d'una metodologia d'anàlisis de riscos: identificació i valoració dels actius, amenaces, vulnerabilitats, càlcul del risc, nivell de risc acceptable i risc residual.

- Fase 4 – Propostes de projectes.

Avaluació de projectes que ha de portar a terme l'organització per alinear-se amb els objectius al Pla Director. Quantificació econòmica i temporal d'aquests.

- Fase 5 – Auditoria de compliment de la ISO.

Avaluació de controls i maduresa i nivell de compliment.

- Fase 6 – Presentació de resultats i lliurament.

Consolidació dels resultats obtinguts durant el procés d'anàlisi. Realització dels informes i presentació executiva a direcció. Entrega del projecte final.

1.4 Planificació del Treball

Per a dur a terme el projecte necessitarem disposar d'una empresa consultora, és a dir, d'un consultor extern a la nostra empresa per realitzar el PDS. Generalment, tota empresa que decideix dur a terme un PDS o bé una revisió d'aquest contracta aquest servei externament. Les empreses que ofereixen aquests serveis solen ser grans empreses.

Per tal d'organitzar les múltiples tasques que exigeix el PDS, hem organitzat el desenvolupament del projecte en sis fases consecutives, on al final de cada fase s'han d'obtenir una sèrie de documents entregables. Com podem veure en el diagrama de Gantt, Figura 1, el projecte comença dia 16 de febrer i finalitza dia 25 de juny. Cada una de les fases té una durada de dues o tres setmanes segons la càrrega de treball que suposa.

Figura 1. Diagrama de Gantt

1.5 Breu sumari de productes obtinguts

Els productes que s'han de presentar com a entregues del projecte i que, per tant, són els productes obtinguts al llarg de la realització d'aquest treball són els que hem especificat a l'apartat anterior i que es poden sintetitzar en els següents:

- Informe d'anàlisi diferencial.
- Esquema documental ISO/IEC 27001.
- Anàlisi de riscs.
- Pla de projectes.
- Auditoria de compliment.
- Presentació dels resultats.

1.6 Breu descripció dels altres capítols de la memòria

La resta de capítols d'aquesta memòria estaran organitzats seguint les cinc primeres fases que s'han detallat a l'apartat de planificació més el capítol de conclusions, el glossari, la bibliografia i els annexos. A continuació detallam els continguts de cada capítol.

- Capítol 2: Contextualització i documentació.
  L'objectiu d'aquest capítol és fitxar i definir les bases de tot el projecte, que en els pròxims capítols desenvoluparem. Primer de tot hem de determinar quin serà el nostre objecte d'estudi, l'empresa en la qual basarem aquest projecte. Llavors realitzar una descripció detallada de l'organització. Després hem de definir l'abast del Pla Director de Seguretat i finalment elaborar una anàlisi de compliment inicial de l'empresa seleccionada.

- Capítol 3: Sistema de gestió documental.
  L'objectiu d'aquest capítol és elaborar la política de seguretat, juntament amb la declaració d'aplicabilitat i la documentació del SGSI. Mitjançant el conjunt de documents que estableix la ISO/IEC 27001 com a necessaris per a poder certificar el sistema obtindrem les bases del nostre SGSI. En aquest capítol tendrem una sèrie d'entregables que són els següents: la política de seguretat, el procediment d'auditories internes, la gestió d'indicadors, el procediment de revisió per direcció, la gestió de rols i responsabilitats, la metodologia d'anàlisis de riscs i la declaració d'aplicabilitat.

- Capítol 4: Estat del risc: identificació i valoració.
  L'objectiu d'aquest capítol és identificar i valorar els actius i les amenaces a les quals està sotmesa la nostra empresa. Això suposa determinar els actius de l'organització, quin valor tenen aquests, avaluar i quantificar les amenaces i avaluar el risc potencial i de l'impacte. En aquest capítol tendrem una sèrie d'entregables que són els següents: una anàlisi detallada dels actius rellevant el nivell de seguretat de l'empresa, un estudi de les possibles amenaces del sistema d'informació

i l'impacte d'aquests i l'avaluació de l'impacte potencial que tendria la materialització de les diferents amenaces a les quals estan exposats els nostres actius.

- Capítol 5: Propostes de projectes.
  L'objectiu d'aquest capítol és fer una avaluació de tots els projectes sorgits a les fases anteriors, que haurà d'implementar l'empresa per poder-se alinear amb els objectius del pla director, realitzant una quantificació econòmica i temporal dels mateixos objectius. En aquest capítol tendrem un únic document entregable que és el pla de projectes.

- Capítol 6: Auditoria de compliment de la ISO.
  L'objectiu d'aquest capítol, i darrer de desenvolupament de continguts del projecte, consisteix en la realització d'una anàlisi de compliment de l'empresa davant la ISO 27001:2013, per tal d'analitzar el control, la maduresa i el nivell de compliment. En aquest capítol tendrem un únic document entregable que és l'informe d'auditoria.

- Capítol 7: Conclusions.
  L'objectiu d'aquest capítol és expressar on hem arribat després d'haver realitzat el treball. Les conclusions han de transmetre una visió panoràmica de tot el treball i cal que donin visibilitat als resultats més importants que s'han aconseguit. És el moment de fer una reflexió crítica sobre l'assoliment dels objectius que ens havíem plantejat a l'inici del treball. A més de fer una anàlisi crítica del seguiment de la planificació i metodologia al llarg del desenvolupament del treball que ens ha permès assolir els objectius. I finalment s'han d'incloure les línies de treball futur que no s'han pogut abordar en la realització d'aquest treball.

- Capítol 8: Glossari.
  En aquest capítol trobarem una llista ordenada alfabèticament dels termes i acrònims, amb les seves definicions, més rellevants que s'han utilitzat al llarg de la redacció d'aquesta memòria.

- Capítol 9: Bibliografia.
  En aquest capítol trobarem recollides totes les fonts i referències bibliogràfiques que s'han citat dins del treball.

- Capítol 10: Annexos.
  En aquest capítol trobarem tot aquell material que no pot col·locar-se en el cos de la memòria, ja que trencaria amb la presentació lògica i ordenada, però que és important que aparegui en la memòria.

2. Contextualització i documentació.

2.1. Descripció detallada de la organització.

L'organització que s'utilitzarà per dur a terme l'estudi i l'anàlisi d'aquest treball de final de màster es basa en una empresa de gestió hotelera. Aquesta empresa és un grup turístic integrat per la divisió hotelera i la divisió de viatges. La filosofia i els valors que desenvolupa l'organització segueixen el perfil d'una empresa familiar, la qual basa la seva activitat en el desenvolupament de negocis turístics.

L'empresa té una dimensió de més de 33.000 persones en plantilla repartides per tot el món. A dia d'avui té més de 250 hotels en vint-i-dos països i més de 700 agències de viatges repartides en quatre continents.

L'empresa en qüestió té les oficines centrals a Palma de Mallorca i oficines secundàries a diferents indrets dels països on es desenvolupa l'activitat. L'oficina central de Palma actualment es divideix amb dos edificis, situats a pocs metres de distància. L'edifici central consta de cinc altures: planta baixa i quatre pisos, la planta baixa hi ha la recepció, el departament de recursos humans, l'oficina regional del mediterrani i el departament de construcció. A la primera planta està ocupada pel departament de tecnologies de la informació. A la segona planta hi trobam el departament de riscs i sinistres i el departament de compres i pagaments. A la tercera planta hi ha el departament de màrqueting i experiència d'usuari i el departament d'innovació. La quarta planta està ocupada pel departament legal, fiscal, auditories i l'oficina del CEO. I finalment a la cinquena planta hi ha el comitè de direcció i la presidència. L'edifici secundari consta només de planta baixa on hi trobam el departament d'ecommerce amb la plataforma de distribució.

Per poder accedir a l'edifici principal cal entrar per l'entrada principal on hi ha personal de seguretat qui controla l'accés al personal autoritzat. En cas de voler accedir al CPD, el qual es troba ubicat a la primera planta de l'edifici central on hi ha el departament d'IT, és necessari disposar d'una targeta magnètica personal i intransferible i la introducció d'un codi personal. A més és necessari emplenar la fulla de registre d'accés ubicada dins del CPD. Per poder accedir a l'edifici secundari és necessari un clauer magnètic personal i intransferible.

A més dels empleats en plantilla de l'empresa, aquesta es complementa amb empreses i personal extern per tal de completar les mancances de certs perfils professionals. Bé perquè no són recursos necessaris diàriament com per exemple per a moments puntuals per algun projecte específic. O bé, perquè econòmicament per l'empresa és millor tenir el servei externalitzat.

A continuació, a la Figura 2, tenim l'organigrama de la nostra empresa, on podem veure com està organitzada l'empresa.

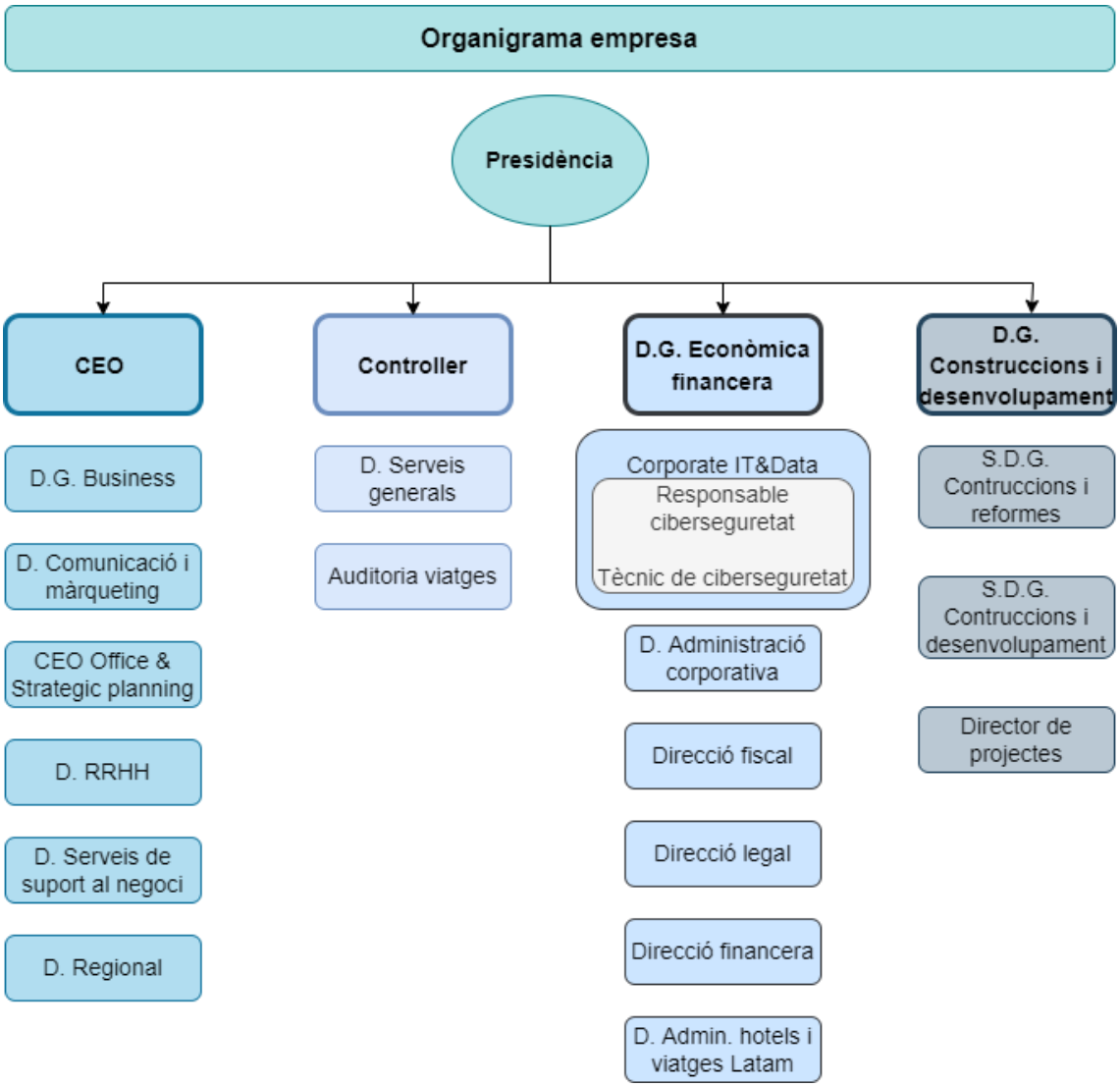


Figura 2. Organigrama de l'empresa

Finalment, podem veure en la Figura 3 el diagrama de xarxa de l'empresa seleccionada com a objecte d'estudi:

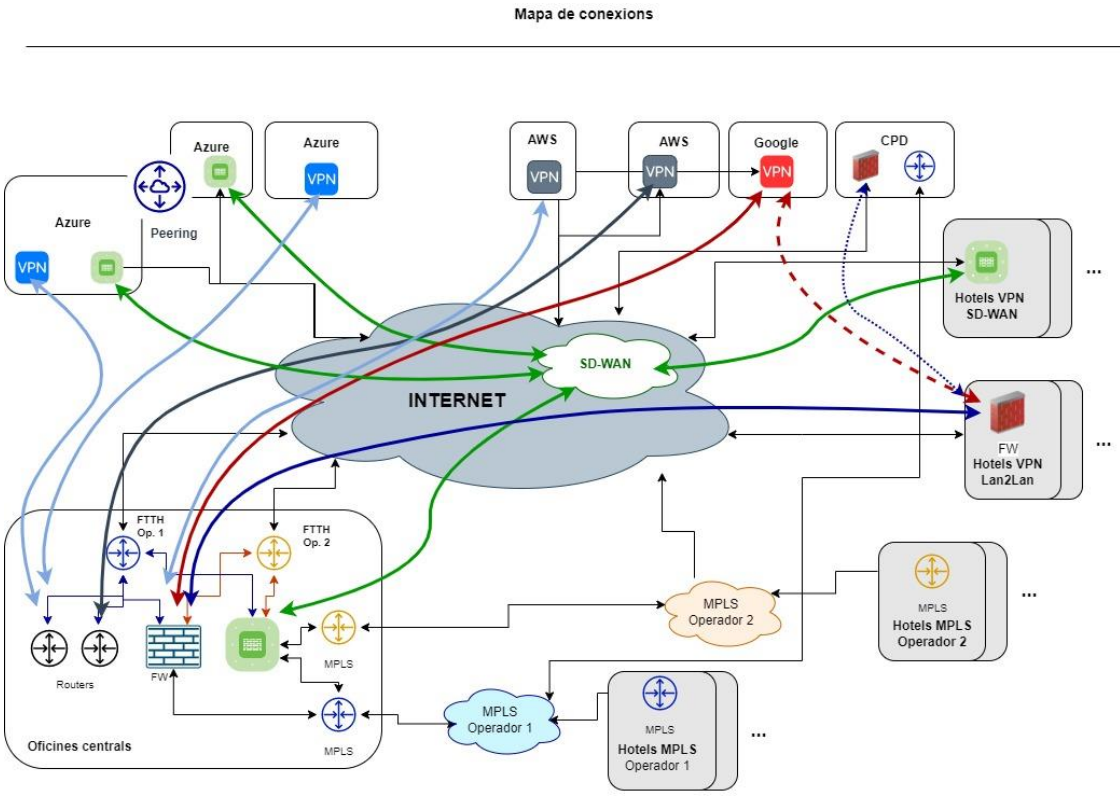


Figura 3. Mapa de connexions de l'empresa

2.2. Abast del pla director de seguretat.

Cada organització o empresa és diferent una de l'altre per això cada una d'elles necessita tenir un Pla Director de Seguretat específic segons quin sigui el seu objectiu estratègic. Per això és essencial definir l'abast sobre el qual desenvoluparem el PDS. L'abast ha de determinar quina és la magnitud de les tasques a realitzar i determinar quin és el focus principal de millora amb l'aplicació del PDS. En el nostre cas, l'abast del pla director és l'oficina central de la divisió hotelera de l'empresa seleccionada. On els processos de negoci que volem protegir són els següents: el procés de venda (e-commerce, venda indirecta, teleoperadors i call center), la informació dels clients, la informació confidencial de l'organització i el software de gestió hotelera. És un objectiu molt ampli on s'han de revisar tots els sistemes de l'empresa i determinar els punts dèbils d'aquesta. Després un cop determinats els punts dèbils cal dur a terme les propostes de millora contínua. Cal mencionar que l'abast inclou tots els actius de l'empresa actuals i futurs. [1]

2.3. Anàlisi de compliment inicial.

Per elaborar l'anàlisi de compliment inicial cal realitzar una anàlisi dels requisits de la norma ISO/IEC 27001:2017 i dels objectius de control que estan definits a l'annex de la normativa i que figuren a la norma ISO/IEC 27002:2017. Per avaluar cada control ho mesurarem mitjançant una aproximació de l'estat de

maduresa dels controls establerts per la normativa, seguint el Model de Maduresa de Capacitat (CMM), que podem veure a la següent taula.

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

Taula 1. Model de Maduresa de la Capacitat (CMM)

Primer de tot començarem amb l'anàlisi dels requisits de la norma ISO/IEC 27001:2017, es pot veure el nivell de compliment per cada un dels controls representat a la Taula 1. [6]

Control	Nivell de compliment
4. Context de l'organització	53%
4.1. Comprensió de l'organització i del seu context	60%

4.2. Comprensió de les necessitats i expectatives de les parts interessades	60%
4.3. Determinació de l'abast del sistema de gestió de la seguretat de la informació	50%
4.4. Sistema de gestió de la seguretat de la informació	40%
5. Lideratge	62%
5.1. Lideratge i compromís	70%
5.2. Política	60%
5.3. Rols, responsabilitats i autoritats en l'organització	55%
6. Planificació	63%
6.1. Accions per tractar els riscs i oportunitats	55%
6.1.1. Consideracions generals	65%
6.1.2. Apreciació del risc de seguretat de la informació	60%
6.1.3. Tractament dels riscs de seguretat de la informació	55%
6.2. Objectius de seguretat de la informació i planificació per la consecució	70%
7. Suport	52%
7.1. Recursos	65%
7.2. Competència	55%
7.3. Conscienciació	35%
7.4. Comunicació	45%
7.5. Informació documentada	60%
7.5.1. Consideracions generals	65%
7.5.2. Creació i actualització	55%
7.5.3. Control de la informació documentada	60%
8. Operació	42%
8.1. Planificació i control operacional	40%
8.2. Apreciació dels riscs de seguretat de la informació	45%
8.3. Tractament dels riscs de seguretat de la informació	40%
9. Avaluació de l'acompliment	67%
9.1. Seguiment, mediació, anàlisi i avaluació.	60%
9.2. Auditoria interna	70%
9.3. Revisió per la direcció	70%
10. Millora	58%
10.1. No conformitat i accions correctives	55%
10.2. Millora continua	60%

Taula 2. Anàlisi dels requisits de la norma ISO/IEC 27001:2017

Un cop analitzats els requisits de la norma ISO/IEC 27001:2017, passam a analitzar els controls de l'annex A de la norma, dels quals es pot veure el nivell de compliment per cada un dels controls representats a la Taula 2. [6]

Control	Nivell de compliment
5. Polítiques de seguretat de la informació	45%
5.1. Directrius de gestió de la seguretat de la informació	45%
5.1.1. Polítiques per la seguretat de la informació	50%
5.1.2. Revisió de les polítiques per la seguretat de la informació	40%
6. Organització de la seguretat de la informació	57%
6.1. Organització interna	56%
6.1.1. Rols i responsabilitats en seguretat de la informació	60%
6.1.2. Segregació de tasques	50%
6.1.3. Contacte amb les autoritats	60%
6.1.4. Contacte amb grups d'interès especial	50%
6.1.5. Seguretat de la informació en la gestió de projectes	60%
6.2. Els dispositius mòbils i el teletreball	58%
6.2.1. Política de dispositius mòbils	50%
6.2.2. Teletreball	65%
7. Seguretat relativa als recursos humans	53%
7.1. Abans del treball	53%
7.1.1. Investigació d'antecedents	40%
7.1.2. Terminis i condicions de l'empleat	65%
7.2. Durant el treball	60%
7.2.1. Responsabilitats de gestió	70%
7.2.2. Conscienciació, educació i capacitació en seguretat de la informació	50%
7.2.3. Procés disciplinari	60%
7.3. Finalització del treball o canvi en el lloc de feina	45%
7.3.1. Responsabilitats davant la finalització o el canvi	45%
8. Gestió d'actius	61%
8.1. Responsabilitat sobre els actius	74%
8.1.1. Inventari d'actius	70%
8.1.2. Propietat dels actius	80%
8.1.3. Ús acceptable dels actius	75%
8.1.4. Devolució d'actius	70%
8.2. Classificació de la informació	68%
8.2.1. Classificació de la informació	65%
8.2.2. Etiquetat de la informació	70%
8.2.3. Manipulació de la informació	70%
8.3. Manipulació de suports extraibles	40%
8.3.1. Gestió de suports extraibles	30%
8.3.2. Eliminació de suports	50%
8.3.3. Suports físics en trànsit	40%
9. Control d'accés	68%

9.1. Requisits de negoci per controlar l'accés	68%
9.1.1. Política de control d'accés	65%
9.1.2. Accés a les xarxes i als serveis de xarxa	70%
9.2. Gestió d'accés d'usuari	62%
9.2.1. Registre i baixa d'usuari	70%
9.2.2. Provisió d'accés de l'usuari	60%
9.2.3. Gestió de privilegis d'accés	80%
9.2.4. Gestió de la informació secreta d'autenticació dels usuaris	60%
9.2.5. Revisió dels drets d'accés d'usuari	60%
9.2.6. Retirada o reassignació dels drets d'accés	40%
9.3. Responsabilitats d'usuari	70%
9.3.1. Ús de la informació secreta d'autenticació	70%
9.4. Control d'accés a sistemes i aplicacions	72%
9.4.1. Restricció d'accés a la informació	80%
9.4.2. Procediments segurs d'inici de sessió	70%
9.4.3. Sistema de gestió de contrasenyes	60%
9.4.4. Ús d'utilitats amb privilegis del sistema	70%
9.4.5. Control d'accés al codi font dels programes	80%
10. Criptografia	55%
10.1. Controls criptogràfics	55%
10.1.1. Política d'ús dels controls criptogràfics	60%
10.1.2. Gestió de claus	50%
11. Seguretat física i de l'entorn	68%
11.1 Àrees segures	79%
11.1.1. Perímetre de seguretat física	80%
11.1.2. Controls físics d'entrada	90%
11.1.3. Seguretat d'oficines, despatxos i recursos	80%
11.1.4. Protecció contra les amenaces externes i ambientals	70%
11.1.5. El treball en àrees segures	75%
11.1.6. Àrees de carrega i descarrega	80%
11.2. Seguretat dels equips	57%
11.2.1. Emplaçament i protecció d'equips	50%
11.2.2. Instal·lacions de subministrament	65%
11.2.3. Seguretat del cablejat	70%
11.2.4. Manteniment dels equips	60%
11.2.5. Retirada de materials propietat de l'empresa	50%
11.2.6. Seguretat dels equips fora de les instal·lacions	50%
11.2.7. Reutilització o eliminació segura dels equips	60%
11.2.8. Equip d'usuari desatengut	50%
11.2.9. Política de lloc de treball buit i pantalla neta	60%
12. Seguretat de les operadores	67%

12.1. Procediments i responsabilitats operacionals	63%
12.1.1. Documentació de procediments de les operacions	70%
12.1.2. Gestió dels canvis	50%
12.1.3. Gestió de les capacitats	60%
12.1.4. Separació dels recursos de desenvolupament, prova i operació	70%
12.2. Protecció contra el software maliciós (malware)	70%
12.2.1. Controls contra el codi maliciós	70%
12.3. Copies de seguretat	80%
12.3.1. Copies de seguretat de la informació	80%
12.4. Registres i supervisió	66%
12.4.1. Registre d'esdeveniments	80%
12.4.2. Protecció de la informació del registre	70%
12.4.3. Registres d'administració i operació	65%
12.4.4. Sincronització del rellotge	50%
12.5. Control del software en explotació	65%
12.5.1. Instal·lació del software en explotació	65%
12.6. Gestió de la vulnerabilitat tècnica	55%
12.6.1. Gestió de les vulnerabilitats tècniques	60%
12.6.2. Restricció en la instal·lació del software	50%
12.7. Consideracions sobre l'auditoria de sistemes d'informació	70%
12.7.1. Controls d'auditoria de sistemes d'informació	70%
13. Seguretat de les comunicacions	58%
13.1. Gestió de la seguretat de xarxes	55%
13.1.1. Controls de xarxa	65%
13.1.2. Seguretat dels serveis de xarxa	60%
13.1.3. Segregació en xarxa	40%
13.2. Intercanvi d'informació	61%
13.2.1. Polítiques i procediments d'intercanvi d'informació	50%
13.2.2. Acords d'intercanvi d'informació	50%
13.2.3. Missatgeria electrònica	60%
13.2.4. Acords de confidencialitat o no revelació	85%
14. Adquisició, desenvolupament i manteniment	67%
14.1. Requisits de seguretat en els sistemes d'informació	68%
14.1.1. Anàlisi de requisits i especificacions de seguretat de la informació	60%
14.1.2. Assegurar els serveis d'aplicacions en xarxes públiques	75%
14.1.3. Protecció de les transaccions de servidors d'aplicacions	70%
14.2. Seguretat en el desenvolupament i en els processos de suport	66%
14.2.1. Política de desenvolupament segur	70%

14.2.2. Procediment de control de canvis en els sistemes	70%
14.2.3. Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu	70%
14.2.4. Restriccions als canvis en els paquets de software	40%
14.2.5. Principis d'enginyeria de sistemes segurs	60%
14.2.6. Entorn de desenvolupament segur	70%
14.2.7. Externalització del desenvolupament de software	70%
14.2.8. Proves funcionals de seguretat de sistemes	70%
14.2.9. Proves d'acceptació de sistemes	70%
14.3. Dades de prova	60%
14.3.1. Protecció de les dades de prova	60%
15. Relació amb els proveïdors	70%
15.1. Seguretat en les relacions amb proveïdors	70%
15.1.1. Política de seguretat de la informació en les relacions amb els proveïdors	70%
15.1.2. Requisits de seguretat en contractes amb tercers	70%
15.1.3. Cadena de subministrament de tecnologia de la informació i de les comunicadores	70%
15.2. Gestió de la provisió dels serveis del proveïdor	70%
15.2.1. Control i revisió de la provisió dels serveis del proveïdor	70%
15.2.2. Gestió de canvis en la provisió del servei del proveïdor	70%
16. Gestió d'incidents de seguretat de la informació	61%
16.1. Gestió d'incidents de seguretat de la informació i millores	61%
16.1.1. Responsabilitats i procediments	60%
16.1.2. Notificació dels esdeveniments de seguretat de la informació	70%
16.1.3. Notificació de punts dèbils de la seguretat	70%
16.1.4. Avaluació i decisió sobre els esdeveniments de seguretat d'informació	60%
16.1.5. Resposta a incidents de seguretat de la informació	60%
16.1.6. Aprenentatge dels incidents de seguretat de la informació	50%
16.1.7. Recopilació d'evidències	60%
17. Aspectes de seguretat de la informació per la gestió de la continuïtat del negoci	63%
17.1. Continuïtat de la seguretat de la informació	57%
17.1.1. Planificació de la continuïtat de la seguretat de la informació	60%
17.1.2. Implementar la continuïtat de la seguretat de la informació	60%
17.1.3. Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació	50%
17.2. Redundàncies	70%

17.2.1. Disponibilitat dels recursos de tractament de la informació	70%
18. Compliment	63%
18.1. Compliment dels requisits legals i contractuals	65%
18.1.1. Identificació de la legislació aplicable dels requisits contractuals	70%
18.1.2. Drets de propietat intel·lectual (DPI)	65%
18.1.3. Protecció dels registres de l'organització	70%
18.1.4. Protecció i privacitat de la informació de caràcter personal	60%
18.1.5. Regulació dels controls criptogràfics	60%
18.2. Revisions de la seguretat de la informació	60%
18.2.1. Revisió independent de la seguretat de la informació	60%
18.2.2. Compliment de les polítiques i normes de seguretat	60%
18.2.3. Comprovació del compliment tècnic	60%

Taula 3. Anàlisi dels controls de l'annex A de la norma ISO 27001:2017

Un cop hem finalitzat l'anàlisi diferencial inicial, representam els valors obtinguts dels requisits de la norma ISO i dels controls de l'annex, respectivament en les gràfiques següents, Figura 4 i 5. La representació es realitza segons el nivell de maduresa percentual dels diferents controls, el que ens dona una visió general de l'estat de seguretat de l'empresa.

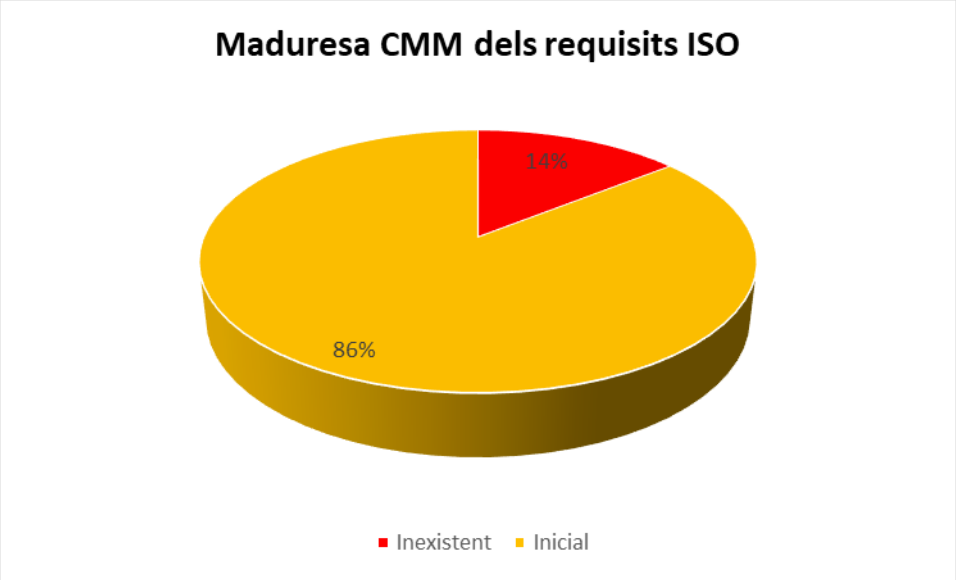


Figura 4. Gràfica de la maduresa dels requisits de la norma ISO

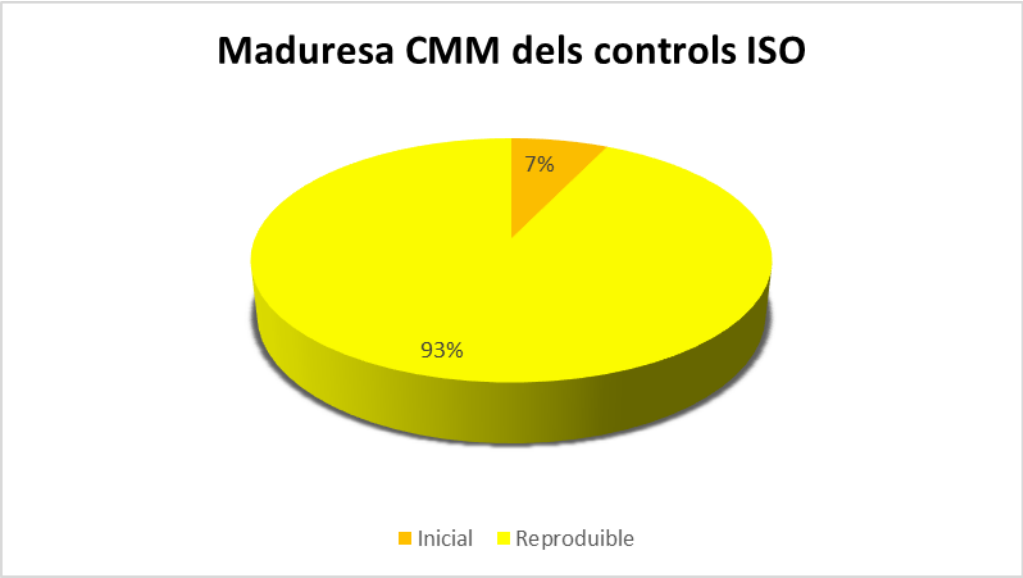


Figura 5. Gràfica de la maduresa dels controls ISO

A continuació per tal de veure els resultats obtinguts de l'anàlisi diferencial segons cada un dels controls, realitzam un diagrama de tipus radar de tots els requisits i controls, Figura 6 i 7 respectivament, per a representar el nivell de compliment de la ISO que té actualment l'empresa.

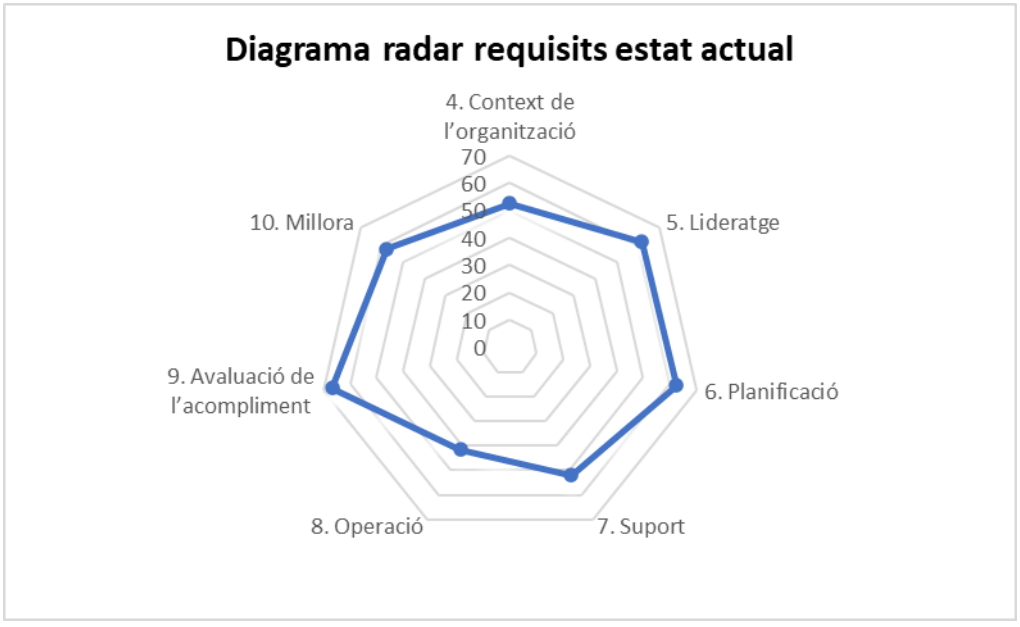


Figura 6. Diagrama radar dels requisits de la norma ISO, estat actual.

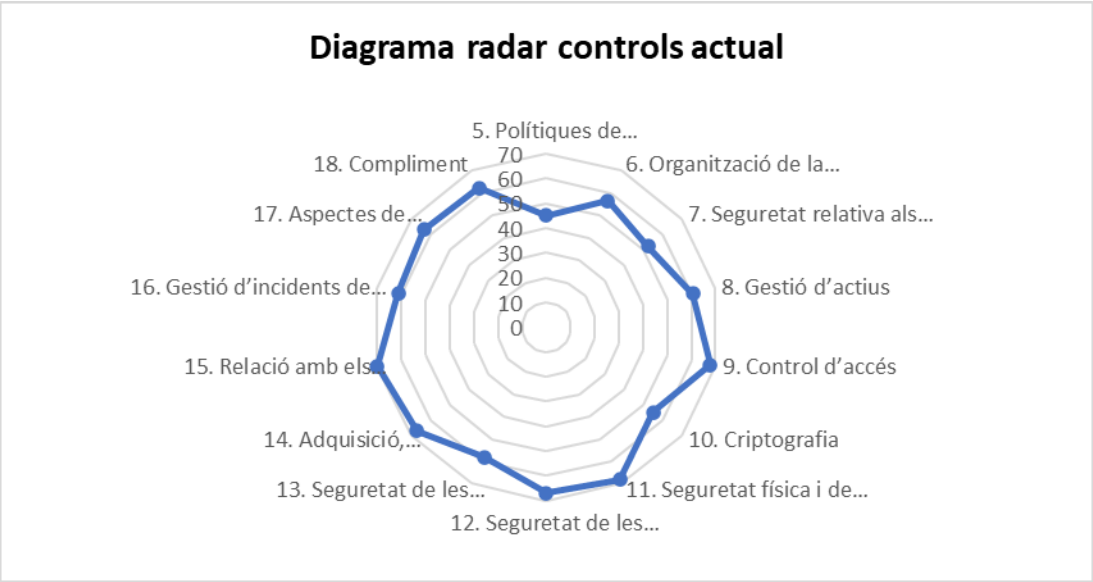


Figura 7. Diagrama radar dels requisits dels controls, estat actual

A més de saber quin és l'estat actual de l'empresa és molt interessant comparar aquests valors amb l'estat que desitjam, per això hem realitzat un altre diagrama de tipus radar, Figura 8 i 9, on podem veure la comparativa dels dos estats, actual i desitjable.

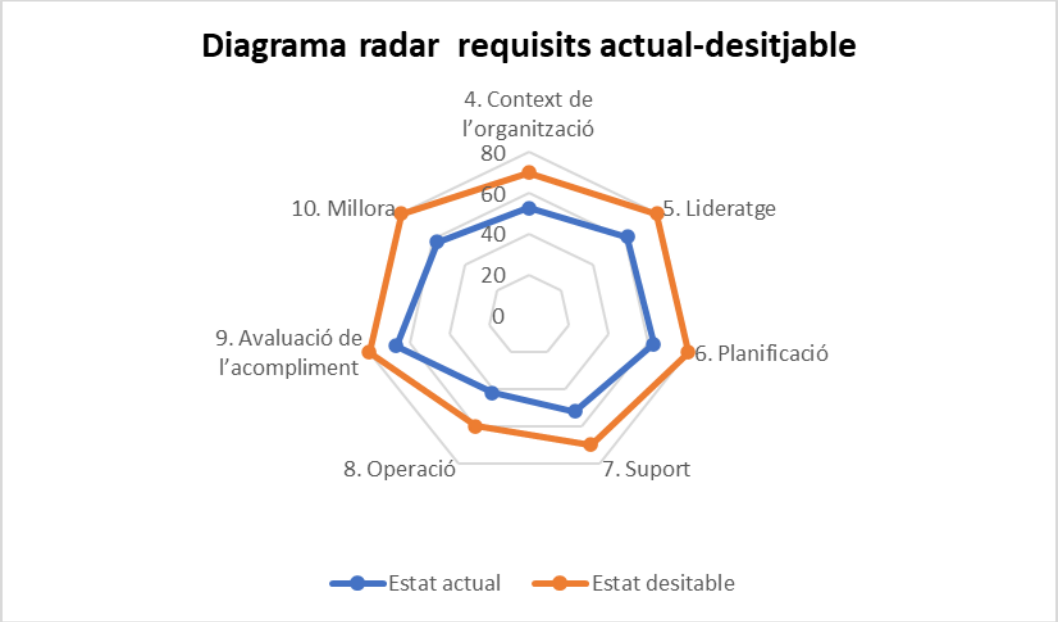


Figura 8. Diagrama radar dels requisits de la norma ISO, estat actual i desitjable

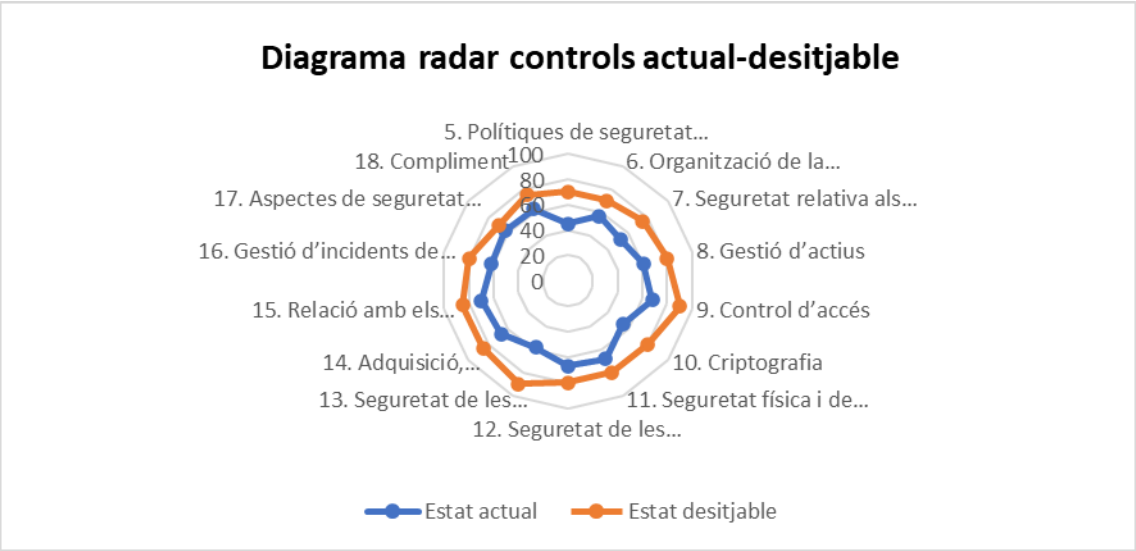


Figura 9. Diagrama radar dels controls, estat actual i desitjable.

3. Sistema de gestió documental

Un sistema de gestió documental és un conjunt de normes, tècniques i pràctiques utilitzades per administrar el flux de documents d'una organització, permetre la recuperació de la informació des d'ells mateixos, determinar el temps que els documents han de guardar-se, eliminar els documents que ja no serveixen i assegurar la conservació indefinida dels documents més valuosos, aplicant principis de racionalització i d'economia.

Tots els sistemes de gestió es basen en un cos documental pel compliment normatiu, el que significa que per al nostre Sistema de Gestió de Seguretat de la Informació (SGSI) hem de tenir en compte els documents que venen establerts per la normativa ISO/IEC 27001, els quals són necessaris per a la certificació del sistema. L'esquema documental està format pels següents documents, els quals veurem en els pròxims apartats d'aquest capítol 3.

- Política de seguretat.
- Procediment d'auditoria interna.
- Gestió d'indicadors.
- Procediment de revisió per direcció.
- Gestió de rols i responsabilitats.
- Metodologia d'anàlisi de riscs.
- Declaració d'aplicabilitat.

3.1. Política de seguretat.

La direcció de l'empresa, acorda que el desenvolupament de les activitats de negoci de l'organització requereix garantir, en tot moment, la confidencialitat, la integritat i la disponibilitat de la informació objecte de tractament a l'organització.

Aquesta política es troba alineada amb el context de l'estratègia de gestió de riscs de l'organització, context en el qual té lloc la creació i el manteniment del Sistema de Gestió de la Seguretat de la Informació (SGSI).

Els objectius són els següents:

1. Fer patent el compromís de la Direcció General en relació amb la seguretat de la informació, acord amb l'estratègia de negoci.
2. Procedir al tractament dels riscos, de manera que han de ser implantats controls que permetin la reducció d'aquests riscos fins al nivell d'acceptació del risc establert per l'organització.
3. Definir, desenvolupar i implantar els controls tècnics i organitzatius que resultin necessaris per a garantir la confidencialitat, integritat i disponibilitat de la informació gestionada a l'empresa.
4. Garantir el compliment de la legislació vigent en matèria de protecció de dades de caràcter personal i societat de la informació, així com de tots

els requeriments legals, reglamentaris i contractuals que resultin aplicables.
5. Crear una “cultura de seguretat” tant internament, en relació amb tot el personal, com externament, en relació amb els clients i proveïdors de l’empresa.
6. Considerar la seguretat de la informació com un procés de millora contínua, que permeti aconseguir nivells de seguretat cada vegada més avançats.

Per tal de garantir aquests objectius de seguretat, s’han desenvolupat normes i procediments de seguretat, on es detallen les mesures tècniques, organitzatives i de gestió necessàries per garantir el compliment de les directrius establertes per la política de seguretat.

A l’Annex 1 d’aquest treball hi trobarem detallada la política de seguretat de l’empresa. [4]

3.2. Procediment d’auditories internes.

Per a qualsevol empresa és essencial implementar un procés d’auditoria interna si es vol realitzar un procés de millora contínua del Sistema de Gestió de la Seguretat de la Informació (SGSI).

A l’Annex 2 d’aquest treball hi trobarem descrit el procés d’auditoria interna. On hi ha una planificació de les auditories que es duran a terme durant un any per tal de complir amb la certificació, juntament amb els requisits i funcionalitats principals que estableixen els auditors interns. I finalment hi trobarem un model d’informe d’auditoria.

3.3. Gestió d’indicadors.

Per a cada un dels controls definits al Sistema de Gestió de Seguretat de la Informació (SGSI) és necessari una mesura d’avaluació per poder avaluar el grau d’implicació del sistema. Per tal de monitorejar i millorar de manera contínua els processos i la gestió TI i obtenir un sistema que estigui dins dels marges desitjables, hem d’avaluar constantment l’eficiència del sistema mitjançant uns indicadors, els quals ens permetin quantificar l’estat del funcionament del sistema segons les mesures de seguretat establertes.

A l’Annex 3 d’aquest treball hi trobarem definits els indicadors per mesurar l’eficiència dels controls de seguretat implantats i la sistemàtica per a fer les mesures. [2]

3.4. Procediment de revisió per direcció.

La revisió per la direcció té com a finalitat principal assegurar la millora contínua i verificar l’adequació i eficàcia del Sistema de Gestió de la Seguretat

de la Informació (SGSI), el funcionament actual, l'anàlisi de dades i la detecció d'oportunitats de millora, per promoure la millora contínua del sistema i de l'organització.

Dur a terme la revisió del sistema per part de la direcció aporta valor a l'empresa, ja que es realitza una anàlisi de la totalitat de la informació del sistema i s'obtenen conclusions sobre l'alineació amb els processos estratègics de l'empresa. És necessari fer la revisió del SGSI per la direcció perquè permet a l'empresa prendre decisions gràcies a la informació que aporta al sistema. Generalment, aquesta revisió del sistema es durà a terme un cop a l'any.

A l'Annex 4 d'aquest treball hi trobarem definida la revisió per part de la direcció, seguint la normativa ISO/IEC 27001.

3.5. Gestió de rols i responsabilitats.

Tot Sistema de Gestió de la Seguretat de la Informació (SGSI) ha d'estar compost per un equip que s'encarregui de crear, mantenir, supervisar i millorar el sistema. Aquest equip de treball és conegut habitualment com a Comitè de Seguretat i està compost com a mínim per una persona del comitè de direcció.

El Comitè de Seguretat és una entitat que està formada pels responsables de cada àrea de l'empresa. En el cas de la nostra empresa, els membres del comitè seran els següents: CEO, responsable de recursos humans, responsable de comunicació i màrqueting, responsable d'IT, responsable de ciberseguretat, responsable financer, responsable fiscal i legal.

A l'Annex 5 d'aquest treball hi trobarem l'organigrama de l'empresa i els diferents rols i responsabilitats.

3.6. Metodologia d'Anàlisis de Riscos

Elaborar una anàlisi de riscos és una activitat essencial per la implementació, manteniment i millora d'un Sistema de Gestió de la Seguretat de la Informació (SGSI), ja que et permet identificar els punts dèbils de l'organització. L'anàlisi de riscos es realitzarà seguint la metodologia MAGERIT (Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes de la Informació), que té per objectiu avaluar, homologar i certificar el SGSI segons la normativa ISO/IEC 27001.

A l'Annex 6 d'aquest treball hi trobarem detallada la metodologia de l'anàlisi de riscos que haurem de seguir. [3] [5]

3.7. Declaració d'aplicabilitat.

La declaració d'aplicabilitat és un document que ens permet establir els controls i les polítiques de la ISO/IEC 27001 que ha d'implementar el sistema per tal de mantenir la informació segura i disponible.

A l’Annex 7 d’aquest treball hi trobarem detallada la declaració d’aplicabilitat de l’organització, on s’indica si aplica i la justificació del control.

4. Anàlisi de riscos

L'anàlisi de riscos consisteix a identificar cadascun dels riscs, la magnitud d'aquests i les àrees relacionades que requereixen implementar mesures de protecció. L'organització ha de reconèixer tots els possibles problemes que poden afectar a la seva informació i determinar la probabilitat d'ocurrència i el seu impacte.

L'anàlisi de riscos es realitzarà seguint la metodologia MAGERIT, la qual tenim descrita a l'Annex 3.

4.1. Inventari d'actius

La primera tasca que hem de realitzar per poder protegir els nostres actius és dur a terme l'estudi dels actius que estan vinculats a la informació. Abans de valorar els actius i les seves amenaces i vulnerabilitats, cal identificar-los.
Per tal de facilitar la realització de l'inventari d'actius, s'ha decidit agrupar els actius per grups i basar-se en la metodologia MAGERIT. [5] Els actius es classificaran en els següents grups:

- Instal·lacions (L): lloc físic on es duen a terme les activitats relacionades amb l'objecte d'anàlisi i on es troben els sistemes d'informació i comunicació.

- Hardware (HW): medis destinats a suportar els serveis que presenta l'organització, on es dipositen les dades i suporta l'execució de les aplicacions informàtiques o responsables dels processos de transmissió de dades.

- Aplicació (SW): aplicacions que gestionen, analitzen i transformen les dades permetent l'explotació de la informació per la prestació dels serveis.

- Dades (D): la informació que està emmagatzemada en els equips o suports d'informació, la qual es transfereix per distints medis.

- Xarxa (COM): instal·lacions dedicades com a serveis de comunicació centrades en els mitjans de transport que porten dades d'un lloc a un altre.

- Serveis (S): funció que satisfà la necessitat dels usuaris del servei.

- Equipament auxiliar (AUX): altres equips que serveixen de suport als sistemes de la informació que no estan directament relacionats amb les dades.

- Personal (P): persones que estan relacionades amb els sistemes de la informació.

El resultat de l'inventari d'actius de la nostra empresa és el següent:

Inventari actius	
Àmbit	[Id] Actiu
Instal·lacions	[L1] Oficines centrals de l'organització
	[L2] CPD
	[L3] Racks
Hardware	[HW1] Ordinadors i pantalles
	[HW2] Portàtils
	[HW3] Telèfons mòbils
	[HW4] Impressores
	[HW5] Servidors
Aplicació / software	[SW1] Sistema operatiu
	[SW2] Sistema de base de dades
	[SW3] Software antivirus
	[SW4] Software desenvolupament
	[SW5] Software de gestió
	[SW6] Navegadors web
	[SW7] Llicències de software empresarial
Dades	[D1] Còpies de seguretat
	[D2] Bases de dades de clients i proveïdors
	[D3] Base de dades personal de l'organització
	[D4] Arxius de configuració
	[D5] Arxius d'identificadors i contrasenyes
Xarxa	[COM1] Xarxa local (LAN)
	[COM2] Xarxa wifi
	[COM3] Xarxa telefònica
	[COM4] Routers
	[COM5] Firewalls
	[COM6] Switch
	[COM7] AP
Serveis	[S1] Servei de correu institucional
	[S2] Servei d'accés a internet
	[S3] Servei de vendes
	[S4] Servei web
Equipament auxiliar	[AUX1] Sistema de comunicacions redundant
Personal	[P1] Treballadors propis
	[P2] Treballadors subcontractats

Taula 4. Inventari d'actius

4.2. Taula de valoracions

Com que l'objectiu final és prendre un conjunt de mesures que garanteixin els nostres actius, cal que el cost de les mesures no superi el cost de l'actiu a protegir. Per això cal que determinem el valor de cada un dels actius de l'organització.
Per a realitzar aquesta valoració ens basarem en l'anàlisi que proposa MAGERIT [5], on es proposa la següent escala per a qualificar el valor dels actius, la magnitud de l'impacte i la magnitud del risc: molt baix (MB), baix (B), mig (M), alt (A) i molt alt (MA).

Valoració dels actius		
Àmbit	Actiu	Valoració
Instal·lacions	[L1] Oficines centrals de l'organització	MA
	[L2] CPD	MA
	[L3] Racks	A
Hardware	[HW1] Ordinadors i pantalles	A
	[HW2] Portàtils	A
	[HW3] Telèfons mòbils	M
	[HW4] Impressores	M
	[HW5] Servidors	A
Aplicació / software	[SW1] Sistema operatiu	A
	[SW2] Sistema de base de dades	A
	[SW3] Software antivirus	A
	[SW4] Software desenvolupament	M
	[SW5] Software de gestió	M
	[SW6] Navegadors web	M
	[SW7] Llicències de software empresarial	A
Dades	[D1] Còpies de seguretat	MA
	[D2] Bases de dades de clients i proveïdors	MA
	[D3] Base de dades personal de l'organització	MA
	[D4] Arxius de configuració	MA
	[D5] Arxius d'identificadors i contrasenyes	MA
Xarxa	[COM1] Xarxa local (LAN)	MA
	[COM2] Xarxa wifi	A
	[COM3] Xarxa telefònica	A
	[COM4] Routers	A
	[COM5] Firewalls	A
	[COM6] Switch	A
	[COM7] AP	A
Serveis	[S1] Servei de correu institucional	MA
	[S2] Servei d'accés a internet	MA
	[S3] Servei de vendes	MA
	[S4] Servei web	MA
Equipament auxiliar	[AUX1] Sistema de comunicacions redundant	A

Personal	[P1] Treballadors propis	A
	[P2] Treballadors subcontractats	A

Taula 5. Valoració dels actius

Segons la metodologia MAGERIT, hem de valorar els actius en funció de la dimensió de la seguretat de la informació afectada. Un cop tenim identificats els actius hem de realitzar la valoració ACIDT d'aquests, on aquesta valoració mesura la criticitat a les dimensions de seguretat de la informació manejada pel procés de negoci de l'organització.

Les dimensions de valoració són les característiques que donen valor a un actiu. Aquestes dimensions s'utilitzen per valorar les conseqüències de la materialització de les amenaces. La valoració que rep un actiu d'una certa dimensió és la mesura del perjudici per l'organització si l'actiu es veu danyat per aquesta dimensió.

Segons MAGERIT defineix les següents cinc dimensions de valoració de la seguretat [5]:

- Disponibilitat (D): les entitats o processos tenen accés als actius corresponents quan ho requereixen.

- Integritat (I): l'actiu no ha estat manipulat de manera no autoritzada.

- Confidencialitat (C): la informació no es posa a disposició ni es revela a altres persones o entitats no autoritzades.

- Autenticitat (A): l'entitat és qui diu ser o bé garanteix la font de la qual procedeixen les dades.

- Traçabilitat (T): les actuacions d'una entitat poden ser imputades exclusivament per la mateixa entitat.

Des del punt de vista de la seguretat, juntament amb la valoració dels actius, s'ha d'indicar quin és l'aspecte de la seguretat més crític. Això serà de gran ajuda al moment de pensar en possibles mesures de prevenció, les salvaguardes, ja que seran enfocades en aquells aspectes que més crítics.

El valor que rebi un actiu pot ser propi o acumulat. El valor propi s'assignarà a la informació, quedant la resta d'actius subordinats a les necessitats d'explotació i protecció de la informació. D'aquesta manera, els actius inferiors en un esquema de dependències acumulen el valor dels actius que es recolzen en ells. Cada actiu d'informació pot tenir un valor diferent de cadascuna de les diferents dimensions per a l'organització que desitgem analitzar.

Per analitzar els actius en funció de les dimensions definides utilitzarem la següent escala per realitzar les valoracions de la nostra organització.

Valoració dimensions de seguretat	
Valor	Criteri
10	Dany molt greu a la organització
7-9	Dany greu a la organització
4-6	Dany important a la organització
1-3	Dany menor a la organització
0	Dany irrellevant a la organització

Taula 6. Valoració dimensions de seguretat

A continuació trobam una taula resum amb les valoracions dels actius i la quantificació d'aquests segons les cinc dimensions.

Valoració dels actius							
Àmbit	Actiu	Valoració	Aspectes crítics				
			A	C	I	D	T
Instal·lacions	[L1] Oficines centrals de l'organització	MA	8	8	7	10	6
	[L2] CPD	MA	8	9	8	10	8
	[L3] Racks	A	0	0	0	6	0
Hardware	[HW1] Ordinadors i pantalles	A	7	7	5	8	5
	[HW2] Portàtils	A	7	7	5	8	5
	[HW3] Telèfons mòbils	M	6	6	5	7	6
	[HW4] Impressores	M	5	5	5	6	0
	[HW5] Servidors	A	7	8	8	8	6
Aplicació / software	[SW1] Sistema operatiu	A	9	8	8	8	6
	[SW2] Sistema de base de dades	A	8	8	9	9	7
	[SW3] Software antivirus	A	7	7	8	8	6
	[SW4] Software desenvolupament	M	6	5	7	7	6
	[SW5] Software de gestió	M	5	5	5	5	5
	[SW6] Navegadors web	M	5	5	5	5	5
	[SW7] Llicències de software empresarial	A	8	6	6	7	5
Dades	[D1] Còpies de seguretat	MA	8	8	9	10	7
	[D2] Bases de dades de clients i proveïdors	MA	7	7	8	9	7
	[D3] Base de dades personal de l'organització	MA	7	7	8	9	7
	[D4] Arxius de configuració	MA	9	8	8	10	8
	[D5] Arxius d'identificadors i contrasenyes	MA	9	8	9	10	8
Xarxa	[COM1] Xarxa local (LAN)	MA	9	8	9	8	7
	[COM2] Xarxa wifi	A	8	7	8	8	3
	[COM3] Xarxa telefònica	A	7	6	7	8	3

	[COM4] Routers	A	6	6	7	8	5
	[COM5] Firewalls	A	6	6	7	8	5
	[COM6] Switch	A	6	6	7	8	5
	[COM7] AP	A	6	6	7	8	5
Serveis	[S1] Servei de correu institucional	MA	8	9	8	9	7
	[S2] Servei d'accés a internet	MA	7	7	8	10	7
	[S3] Servei de vendes	MA	8	7	8	10	7
	[S4] Servei web	MA					
Equipament auxiliar	[AUX1] Sistema de comunicacions redundant	A	8	7	7	8	3
Personal	[P1] Treballadors propis	A	0	0	8	9	0
	[P2] Treballadors subcontractats	A	0	0	8	8	6

Taula 7. Resum valoració actius i dimensions

4.3. Anàlisi d'amenaces

Tot actiu està exposat a amenaces, les quals poden afectar a diferents aspectes de la seguretat. Per tal de realitzar una estimació de les vulnerabilitats de cada actiu davant la materialització d'una amenaça es durà a terme una anàlisi d'amenaces on s'ha de tenir en compte la freqüència en la qual poden ocórrer aquestes amenaces i l'impacte que tendria en la seguretat de l'organització en cas que aquest es materialitzés. Un cop més ens basam en la metodologia de MAGERIT que estableix una classificació de les possibles amenaces que poden esdevenir sobre els actius d'un sistema d'informació. [5] Les amenaces es poden classificar segons el seu origen de la següent manera:

- Desastres naturals (N): successos que poden ocórrer sense intervenció de l'ésser humà com a causa directa o indirecte.

- D'origen industrial (I): successos que poden ocórrer de manera accidental, derivats de l'activitat humans de tipus industrial. Aquesta amenaça pot ocórrer de manera accidental o deliberada.

- Errors i fallides no intencionats (E): falla no intencionada causada per persones, estan alineats amb atacs deliberats.

- Atacs intencionats (A): falla deliberada causada per les persones.

Quan un actiu és víctima d'una amenaça, no l'afecta a totes les seves dimensions, ni amb la mateixa quantitat. Una vegada s'ha determinat l'amenaça que pot perjudicar a un actiu, s'ha de valorar per a cada actiu la freqüència en què es pot produir l'amenaça i el seu impacte en les diferents dimensions de la seguretat de l'actiu.

MAGERIT ha definit la següent taula de probabilitats, Taula 8.

Probabilitat d'ocurrència de les amenaces			
Probabilitat	Valor	Descripció	Periodicitat
MA	100	Molt freqüent	A diari
A	10	Freqüent	Mensual
M	1	Normal	Un cop a l'any
B	1/10	Poc freqüent	Cada varis anys
MB	1/100	Molt poc freqüent	Segles

Taula 8. Probabilitat d'ocurrència de les amenaces

De la mateixa manera MAGERIT ha definit una fracció en termes de percentatges per determinar la degradació de l'actiu un cop s'ha materialitzat l'amenaça, la qual trobam a la següent taula, Taula 9.

Valoració dels impactes		
Impacte	Valor	Descripció
MA	100%	Molt freqüent
A	75%	Freqüent
M	50%	Normal
B	20%	Poc freqüent
MB	5%	Molt poc freqüent

Taula 9. Valoració dels impactes

Ara que ja coneixem els paràmetres de probabilitat d'ocurrència de les amenaces i els de la valoració dels impactes, ja podem determinar per cada tipus d'actiu la freqüència amb la qual es pot produir l'amenaça, així com el seu impacte a les diferents dimensions de la seguretat de l'actiu.

Actius i dimensions de seguretat de les amenaces							
Amenaça	Actiu	Freqüència	Aspectes crítics (%)				
			A	C	I	D	T
Desastre natural (N)							
N.1- Foc	[HW] Hardware	B				75	
	[AUX] Equipament auxiliar	B				25	
	[L] Instal·lacions	B				50	
N.2- Danys per aigua	[HW] Hardware	B				75	
	[AUX] Equipament auxiliar	B				5	
	[L] Instal·lacions	B				50	
N.*- Desastre natural	[HW] Hardware	MB				75	
	[AUX] Equipament auxiliar	MB				5	
	[L] Instal·lacions	MB				50	
D'origen industrial (I)							
I.1- Foc	[HW] Hardware	M				75	
	[AUX] Equipament auxiliar	M				5	
	[L] Instal·lacions	M				50	

I.2- Dany per aigua	[HW] Hardware	B				75	
	[AUX] Equipament auxiliar	B				5	
	[L] Instal·lacions	B				50	
I.3- Contaminació mecànica	[HW] Hardware	M				75	
	[AUX] Equipament auxiliar	M				25	
I.4- Contaminació electromagnètica	[HW] Hardware	MB				50	
	[AUX] Equipament auxiliar	MB				5	
I.5- Averia d'origen físic o lògic	[SW] Software	B				75	
	[HW] Hardware	B				75	
	[AUX] Equipament auxiliar	MB				5	
I.6- Tall de subministrament elèctric	[HW] Hardware	MB				75	
	[AUX] Equipament auxiliar	MB				5	
I.7- Condicions inadequades de temperatura o humitat	[HW] Hardware	B				50	
	[AUX] Equipament auxiliar	B				5	
I.8- Falla del servei de comunicacions	[COM] Xarxa	B				75	
I.9- Interrupció d'altres serveis i subministres essencials	[AUX] Equipament auxiliar	B				50	
I.11- Emanacions electromagnètiques	[HW] Hardware	MB				50	
	[AUX] Equipament auxiliar	MB				5	
	[L] Instal·lacions	MB				25	
Errors i falles no intencionades (E)							
E.1- Errors dels usuaris	[D] Dades	A		75	75	75	
	[S] Serveis	A		25	75	25	
	[SW] Aplicacions	A		50	75	50	
E.2- Errors de l'administrador	[D] Dades	B		50	75	75	
	[S] Serveis	B		25	25	25	
	[SW] Aplicacions	B		25	50	50	
	[HW] Hardware	B		50	50	50	
	[COM] Xarxa	B		25	25	50	
E.4- Errors de configurac	[D] Dades	MB			50		

ió							
E.7- Deficiències en la organització	[P] Personal	B				50	
E.8- Difusió de software maligne	[SW] Software	B		50	75	50	
E.9- Errors de re-encaminament	[S] Serveis	MB		25			
	[SW] Aplicacions	MB		50			
	[COM] Xarxes	MB		50			
E.10- Errors de seqüència	[S] Serveis	MB			25		
	[SW] Software	MB			25		
	[COM] Xarxa	MB			25		
E.15- Alteració accidental de la informació	[D] Dades	B			75		
	[S] Serveis	B			25		
	[SW] Software	B			50		
	[COM] Xarxa	B			50		
	[L] Instal·lacions	B			25		
E.18- Destrucció d'informació	[D] Dades	MB					
	[S] Serveis	MB					
	[SW] Software	MB					
	[COM] Xarxa	MB					
	[L] Instal·lacions	MB					
E.19- Fuga d'informació	[D] Dades	B		75			
	[S] Serveis	B		25			
	[SW] Software	B		50			
	[COM] Xarxa	B		50			
	[L] Instal·lacions	B		25			
	[P] Personal	B		25			
E.20- Vulnerabilitats dels programes (software)	[SW] Software	MB		50	75	50	
E.21- Errors de manteni-ment/actualització de programes (software)	[SW] Software	MB			50	50	
E.23- Errors de manteni-	[HW] Hardware	MB				50	
	[AUX] Equipament auxiliar	MB				50	

ment/actualització d'equips (hardware)							
E.24- Caiguda del sistema per esgotament de recursos	[S] Serveis	MB				25	
	[HW] Hardware	MB				50	
	[COM] Xarxa	MB				50	
E.25- Pèrdua d'equips	[HW] Hardware	MB		75		50	
	[AUX] Equipament auxiliar	MB		25		25	
E.28- Indisposició del personal	[P] Personal	M				75	
Atacs intencionats (A)							
A.5- Suplantació de la identitat de l'usuari	[D] Dades	MB	75	95	75		
	[S] Serveis	MB	25	25	25		
	[SW] Software	MB	50	75	50		
	[COM] Xarxa	MB	50	50	50		
A.6- Abús de privilegi d'accés	[D] Dades	B	75	75	75		
	[S] Serveis	B	25	25	25		
	[SW] Software	B	50	75	50		
	[HW] Hardware	B	50	50	50		
	[COM] Xarxa	B	50	50	50		
A.7- Ús no previst	[S] Serveis	B		25	25	25	
	[SW] Software	B		50	25	50	
	[HW] Hardware	B		50	25	50	
	[COM] Xarxa	B		25	25	50	
	[AUX] Equipament auxiliar	B		25	25	25	
	[L] Instal·lacions	B		25	25	25	
A.8- Difusió de software nociu	[SW] Software	MB		50	75	75	
A.9- Re-encaminament de missatges	[S] Serveis	MB		25			
	[SW] Software	MB		75			
	[COM] Xarxa	MB		50			
A.10- Alteració de seqüència	[S] Serveis	MB			25		
	[SW] Software	MB			50		
	[COM] Xarxa	MB			50		
A.11- Accés no autoritzat	[D] Dades	MB		50	95		
	[S] Serveis	MB		25	25		

	[SW] Software	MB		50	75		
	[HW] Hardware	MB		50	75		
	[COM] Xarxa	MB		50	75		
	[AUX] Equipament auxiliar	MB		25	50		
	[L] Instal·lacions	MB		50	50		
A.12- Anàlisi de trànsit	[COM] Xarxa	MB		75			
A.13- Repudi	[S] Serveis	B			75		
A.14- Intercepció de la informació (escolta)	[COM] Xarxes	MB		95			
A.15- Modificació deliberada de la informació	[D] Dades	MB			50		
	[S] Serveis	MB			25		
	[SW] Software	MB			75		
	[COM] Xarxa	MB			75		
	[L] Instal·lacions	MB			25		
A.18- Destrucció de la informació	[D] Dades	MB				50	
	[S] Serveis	MB				25	
	[SW] Software	MB				50	
	[L] Instal·lacions	MB				25	
A.19- Divulgació de la informació	[D] Dades	B		50			
	[S] Serveis	B		25			
	[SW] Software	B		75			
	[COM] Xarxa	B		75			
	[L] Instal·lacions	B		50			
A.22- Manipulació de programes	[SW] Software	MB		75	75	50	
A.23- Manipulació dels equips	[HW] Hardware	MB		75		50	
	[AUX] Equipament auxiliar	MB		50		35	
A.24- Denegació de servei	[S] Serveis	B				25	
	[HW] Hardware	B				75	
	[COM] Xarxa	B				75	
A.25- Robatori	[HW] Hardware	MB		50		50	
	[AUX] Equipament auxiliar	MB		50		50	
A.26- Atac destructiu	[HW] Hardware	MB				50	
	[AUX] Equipament auxiliar	MB				50	
	[L] Instal·lacions	MB				75	

A.27-Ocupació enemiga	[L] Instal·lacions	MB		75		75	
A.28-Indisponibilitat del personal	[P] Personal	B				50	
A.29-Extorsió	[P] Personal	MB		50	75	50	
A.30-Enginyeria social	[P] Personal	B		75	75	75	

Taula 10. Valoració d'actius i dimensions de seguretat de les amenaces

4.4. Avaluacions d'impacte i probabilitat

L'impacte potencial és la mesura del dany sobre l'actiu derivat de la materialització d'una amenaça. Coneixent el valor dels actius, en diferents dimensions, i la degradació que suposen les amenaces, és directe derivar l'impacte que aquestes tendrien sobre el sistema. Es tracta d'una dada rellevant, ja que permetrà prioritzar el pla d'acció, i a la vegada avaluar com es veu modificat el nomenat valor un con s'apliquen les contramesures.

Per determinar el cost que implicaria per l'organització que es materialitzin les amenaces realitzam la següent estimació, a partir de l'escala de valors definida anteriorment de les dimensions dels actius, Taula 6, en l'escala de 0 a 10 segons el nivell del dany que suposaria. [5]

Valoració impacte potencial							
Àmbit	Actiu	Valoració risc	Aspectes crítics				
			A	C	I	D	T
Instal·lacions	[L1] Oficines centrals de l'organització	A				8	
	[L2] CPD	MA				10	
	[L3] Racks	A				8	
Hardware	[HW1] Ordinadors i pantalles	M		6	4	8	
	[HW2] Portàtils	M		6	5	6	
	[HW3] Telèfons mòbils	M		6	5	4	
	[HW4] Impressores	M		4	4	5	
	[HW5] Servidors	A		6	8	8	
Aplicació / software	[SW1] Sistema operatiu	A	7	5	8	8	6
	[SW2] Sistema de base de dades	A	7	6	9	8	6
	[SW3] Software antivirus	M			7	6	
	[SW4] Software desenvolupament	M		5	7	7	
	[SW5] Software de gestió	B		5	5	5	
	[SW6] Navegadors web	B	4		5	5	

	[SW7] Llicències de software empresarial	M	7	5	6	7	
Dades	[D1] Còpies de seguretat	A		8	9	10	
	[D2] Bases de dades de clients i proveïdors	A		7	8	9	
	[D3] Base de dades personal de l'organització	A		7	8	9	
	[D4] Arxius de configuració	MA	9	8	8	10	
	[D5] Arxius d'identificadors i contrasenyes	MA	9	8	9	10	
Xarxa	[COM1] Xarxa local (LAN)	MA		8	9	8	
	[COM2] Xarxa wifi	A		5	8	8	5
	[COM3] Xarxa telefònica	A		6	7	8	
	[COM4] Routers	M	5	6	7	8	5
	[COM5] Firewalls	M	5	6	7	8	5
	[COM6] Switch	M	5	6	7	8	5
	[COM7] AP	M	5	6	7	8	5
Serveis	[S1] Servei de correu institucional	MA	9	9	9	9	9
	[S2] Servei d'accés a internet	MA	7	7	8	10	7
	[S3] Servei de vendes	MA	8	7	8	10	7
	[S4] Servei web	MA		5	7	7	
Equipament auxiliar	[AUX1] Sistema de comunicacions redundant	M	6	6	6	8	
Personal	[P1] Treballadors propis	A			8	9	
	[P2] Treballadors subcontractats	A			8	8	6

Taula 11. Valoració impacte potencial

Segons MAGERIT, es defineix el risc potencial com aquella mesura del dany probable sobre un sistema. Coneixent l'impacte d'amenaces sobre els actius, és directe derivar el risc tenguent en compte la probabilitat d'ocurrència. El risc augmenta amb l'impacte i la probabilitat. Conèixer el risc potencial ens permet establir un llindar de risc, el qual és necessari definir per decidir si assumim o no un risc i, per tant, aplicar els controls. Tot el que estigui per sota del risc definit com a acceptable, no suposarà una amenaça important per la nostra organització. En canvi, si el nivell del risc és superior al nivell acceptable, haurem d'establir controls per reduir-lo. El nivell de risc acceptable és aprovat per la direcció de l'organització, la qual ha decidit que en termes generals el llindar de risc acceptable és un nivell mitjà. Hi pot haver excepcions en les quals és millor acceptar un nivell alt que la repercussió econòmica que suposa disminuir el nivell del risc a un nivell mitjà. A més hi pot haver altres excepcions, on s'accepta el risc actual perquè hi ha plans de futur per modificar l'actiu, on compensa durant un temps determinat acceptar el nivell de risc per després canviar-ho, com és el cas del CPD, on hi ha una previsió d'eliminar el CPD local i muntar-lo al cloud.

MAGERIT ha definit la següent taula de valoració del risc, Taula 12, per determinar el risc segons la probabilitat i l'impacte.

		Impacte				
		Molt baix	Baix	Mig	Alt	Molt alt
Probabilitat	Molt baix	MB	MB	B	M	M
	Baix	MB	B	M	M	M
	Mig	M	M	M	A	A
	Alt	M	M	A	A	MA
	Molt alt	M	A	A	MA	MA

Taula 12. Valoració del risc

A continuació a la Taula 13, tenim la taula resum dels riscos que afecten als actius de l'organització, els quals s'han calculat a partir de la relació de la probabilitat i l'impacte de la Taula 12.

Valoració risc potencial			
Àmbit	Actiu	Valoració	Descripció
Instal·lacions	[L1] Oficines centrals de l'organització	5	Mig
	[L2] CPD	8	Alt
	[L3] Racks	7	Alt
Hardware	[HW1] Ordinadors i pantalles	5	Mig
	[HW2] Portàtils	5	Mig
	[HW3] Telèfons mòbils	5	Mig
	[HW4] Impressores	3	Mig
	[HW5] Servidors	4	Mig
Aplicació / software	[SW1] Sistema operatiu	9	Alt
	[SW2] Sistema de base de dades	10	Alt
	[SW3] Software antivirus	10	Alt
	[SW4] Software desenvolupament	9	Alt
	[SW5] Software de gestió	9	Alt
	[SW6] Navegadors web	6	Mig
	[SW7] Llicències de software empresarial	5	Mig
Dades	[D1] Còpies de seguretat	8	Alt
	[D2] Bases de dades de clients i proveïdors	6	Mig
	[D3] Base de dades personal de l'organització	6	Mig
	[D4] Arxius de configuració	10	Alt
	[D5] Arxius d'identificadors i contrasenyes	10	Alt
Xarxa	[COM1] Xarxa local (LAN)	9	Alt
	[COM2] Xarxa wifi	7	Alt

	[COM3] Xarxa telefònica	7	Alt
	[COM4] Routers	7	Alt
	[COM5] Firewalls	7	Alt
	[COM6] Switch	7	Alt
	[COM7] AP	7	Alt
Serveis	[S1] Servei de correu institucional	9	Alt
	[S2] Servei d'accés a internet	8	Alt
	[S3] Servei de vendes	9	Alt
	[S4] Servei web	6	Mig
Equipament auxiliar	[AUX1] Sistema de comunicacions redundant	5	Mig
Personal	[P1] Treballadors propis	8	Alt
	[P2] Treballadors subcontractats	8	Alt

Taula 13. Taula resum valoració risc potencial

5. Proposta de projectes

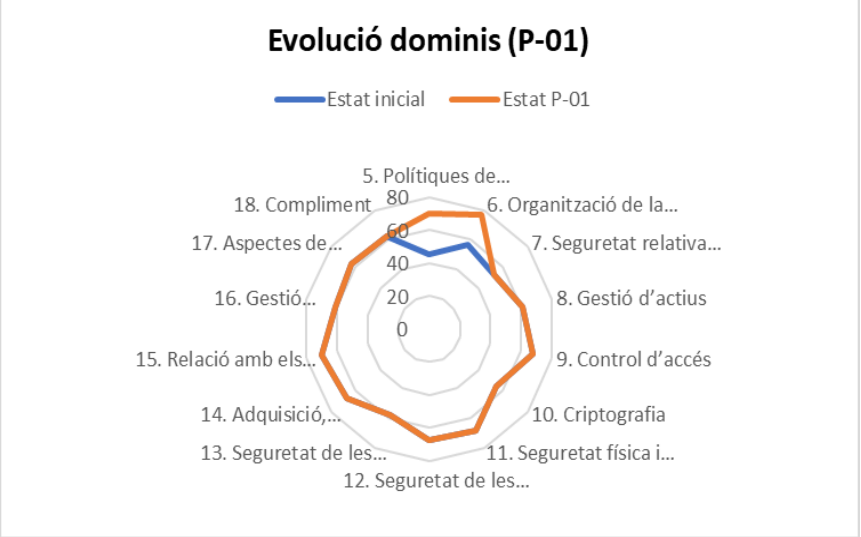
Després de realitzar l'anàlisi de risc ja coneixem el nivell de risc actual de l'organització i és el moment de plantejar-se els projectes per millorar l'estat de la seguretat, és a dir, mitigar el risc actual de l'organització i evolucionar el compliment de la ISO 27001 fins a tenir un nivell acceptable.

La proposta de projectes que veurem a continuació sorgeix a partir de l'anàlisi de risc realitzat anteriorment, on es proposaran aspectes a millorar segons la complexitat i la prioritat de la implementació d'aquests.

Cada projecte que es proposa està detallat amb l'identificador del projecte, el nom del projecte, la categoria a la qual pertany, l'objectiu, la responsabilitat del projecte, la prioritat que té, la planificació temporal, els dominis de la ISO afectats, el cost o pressupost, els riscos a mitigar i un diagrama de tipus radar.

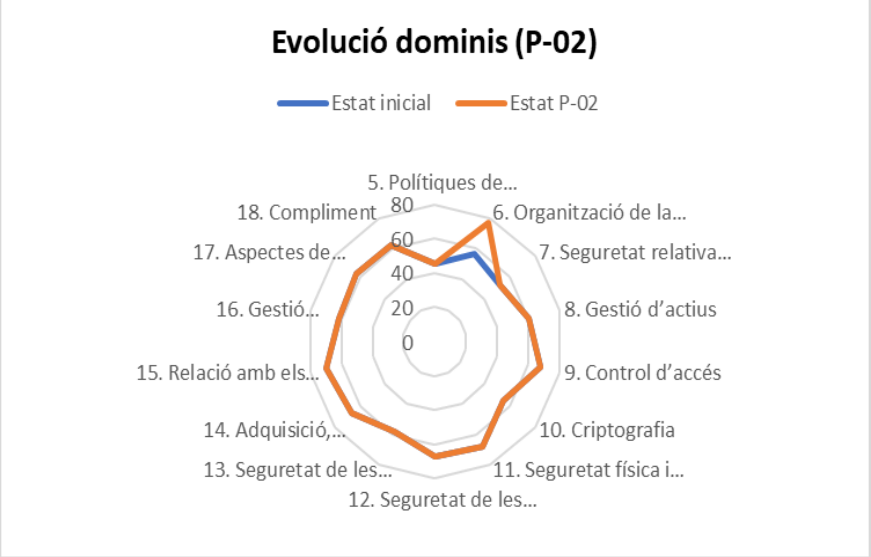
A continuació trobam detallats els projectes proposats que es pretenen realitzar durant el següent any, temps que es tarda a realitzar una revisió completa al SGSI.

ID del projecte	P-01
Nom del projecte	Definició de catàleg de serveis i mapa de processos de l'àrea de seguretat
Categoria	Organització de seguretat
Objectiu	Amb el catàleg de serveis es pretén reunir una llista de serveis i recursos de tal manera que els equips de TI puguin generar informes, analitzar la demanda dels serveis per optimitzar l'oferta i augmentar la satisfacció del client. I amb el mapa de processos es pretén representar amb un inventari gràfic els processos de l'organització per tal de consolidar i validar el consell d'administració de l'empresa
Responsabilitat	Departament de seguretat
Prioritat	Alta
Planificació	Quick win
Dominis ISO	A.05 Polítiques de seguretat A.06 Organització de seguretat de la informació
Cost	6.000 €
Riscos a mitigar	E.1- Errors dels usuaris E.2- Errors de l'administrador E.4- Errors de configuració E.15- Alteració accidental de la informació E.20- Vulnerabilitats dels programes (software) A.7- Ús no previst A.8- Difusió de software nociu A.11- Accés no autoritzat A.24- Denegació de servei

Diagrama radar	

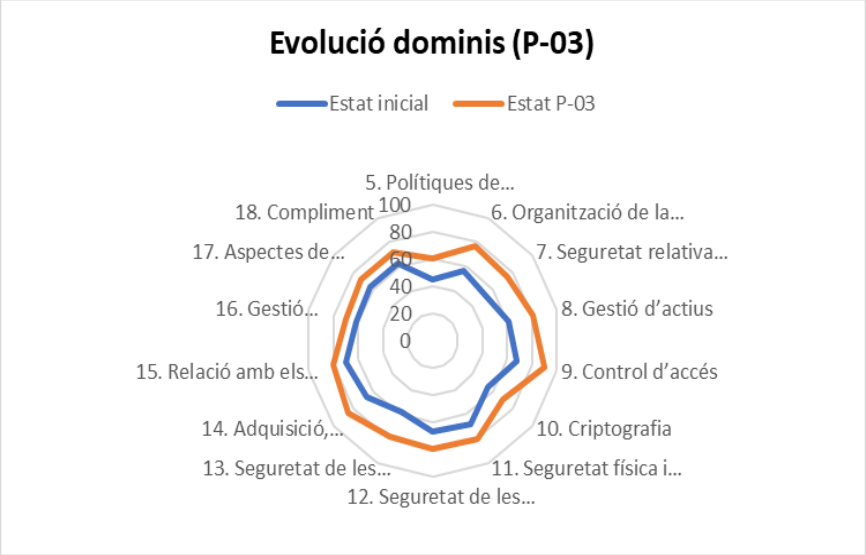
Taula 14. Projecte de millora P-01

ID del projecte	P-02
Nom del projecte	Formalització de la participació de seguretat en la metodologia de gestió de nous projectes de TI.
Categoria	Organització de seguretat
Objectiu	Definir la participació dels treballadors en la gestió de nous projectes de TI després d'haver realitzat enquestes i entrevistes als treballadors de l'organització i haver vist el seu nivell de participació i d'interès en el SGSI
Responsabilitat	Departament de seguretat / IT
Prioritat	Mitjana
Planificació	Quick win
Dominis ISO	A.06 Organització de seguretat de la informació
Cost	6.400 €
Riscos a mitigar	E.1- Errors dels usuaris E.2- Errors de l'administrador E.21- Errors de manteniment/actualització de programes (software) E.23- Errors de manteniment/actualització d'equips (hardware) E.28- Indisposició del personal A.5- Suplantació de la identitat de l'usuari A.6- Abús de privilegi d'accés A.7- Ús no previst A.11- Accés no autoritzat A.24- Denegació de servei A.28- Indisponibilitat del personal A.29- Extorsió

Diagrama radar	

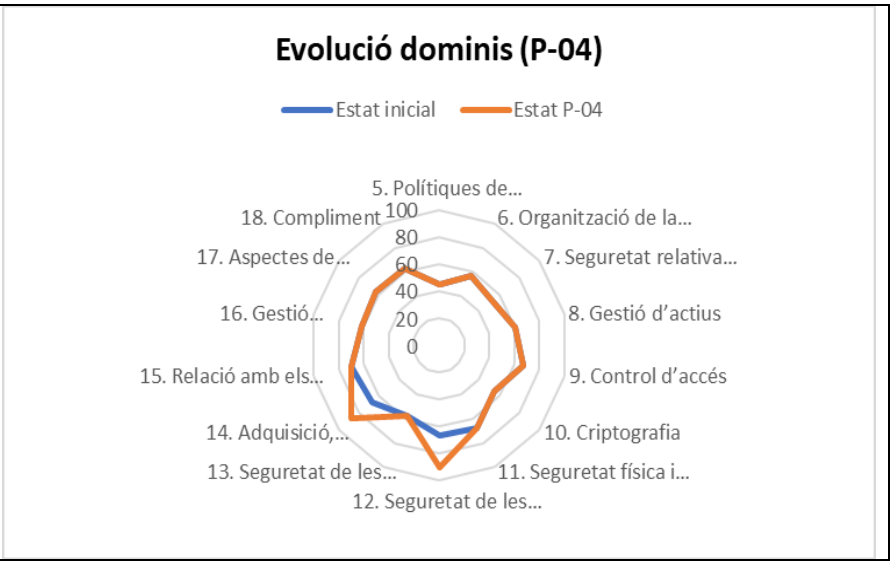
Taula 15. Projecte de millora P-02

ID del projecte	P-03
Nom del projecte	Definició d'un pla de conscienciació i revisió de les capacitats dels usuaris de l'organització.
Categoria	Conscienciació
Objectiu	Amb la definició del pla de conscienciació es pretén reduir les possibilitats d'atac de l'organització, capacitar als usuaris perquè assumeixin la responsabilitat personal de protegir la informació de l'organització i fer complir les polítiques i els procediments que ha implementat l'organització per protegir la seva informació
Responsabilitat	Departament de seguretat
Prioritat	Mitjana
Planificació	Quick win
Dominis ISO	A.05 Polítiques de seguretat A.06 Organització de seguretat de la informació A.07 Seguretat relativa als recursos humans A.08 Gestió d'actius A.09 Control d'accés A.10 Criptografia A.11 Seguretat física i de l'entorn A.12 Seguretat de les operacions A.13 Seguretat de les comunicacions A.14 Adquisició, desenvolupament i manteniment de sistemes A.15 Relacions amb proveïdors A.16 Gestió d'incidents de seguretat de la informació A.17 Continuïtat de negoci A.18 Compliment
Cost	6.800 €
Riscos a mitigar	E.8- Difusió de software maligne E.9- Errors de reencaminament E.19- Fuga d'informació

	E.20- Vulnerabilitats dels programes (software) E.24- Caiguda del sistema per esgotament de recursos A.8- Difusió de software nociu A.10- Alteració de seqüència A.14- Intercepció de la informació (escolta) A.15- Modificació deliberada de la informació A.24- Denegació de servei
Diagrama radar	

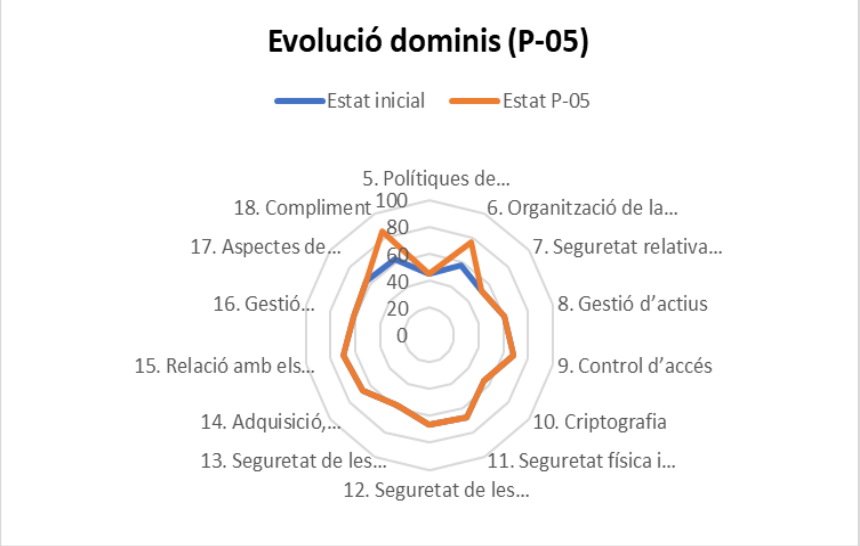
Taula 16. Projecte de millora P-03

ID del projecte	P-04
Nom del projecte	Definició d'un procés de gestió de pegats de seguretat i actualització de sistemes
Categoria	Bastionat
Objectiu	Solucionar possibles vulnerabilitats de seguretat i altres problemes mitjançant les actualitzacions de codi.
Responsabilitat	Departament de seguretat / IT
Prioritat	Alta
Planificació	Quick win
Dominis ISO	A.12 Seguretat de les operacions A.14 Adquisició, desenvolupament i manteniment de sistemes
Cost	8.000 €
Riscos a mitigar	E.2- Errors de l'administrador E.4- Errors de configuració E.21- Errors de manteniment/actualització de programes (software) E.23- Errors de manteniment/actualització d'equips (hardware) E.24- Caiguda del sistema per esgotament de recursos A.8- Difusió de software nociu A.22- Manipulació de programes A.23- Manipulació dels equips

Diagrama radar	

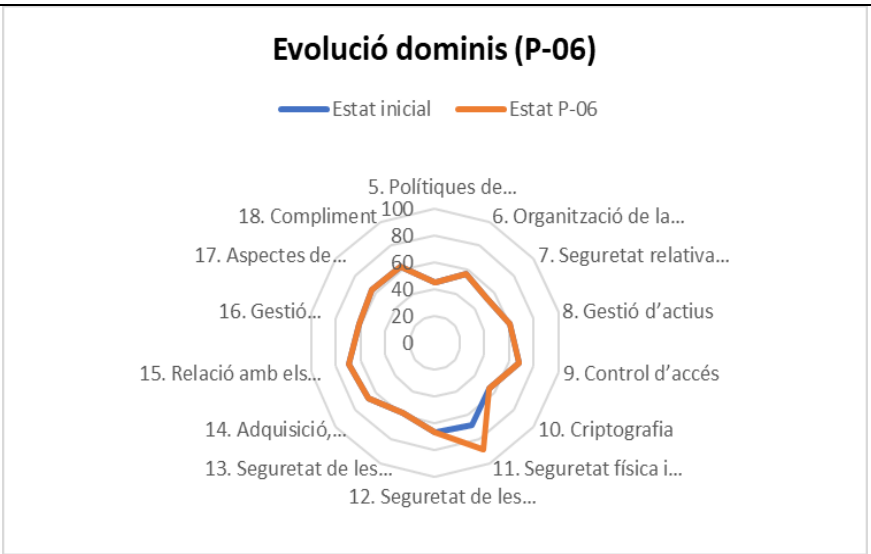
Taula 17. Projecte de millora P-04

ID del projecte	P-05
Nom del projecte	Definició del pla d'auditoria de seguretat de la informació
Categoria	Auditories de seguretat
Objectiu	Crear un marc prou detallat perquè qualsevol auditor extern sigui capaç d'entendre les proves que s'han realitzat
Responsabilitat	Departament de seguretat
Prioritat	Mitjana
Planificació	Quick win
Dominis ISO	A.06 Organització de seguretat de la informació A.18 Compliment
Cost	4.000 €
Riscos a mitigar	E.7- Deficiències en l'organització E.15- Alteració accidental de la informació E.18- Destrucció d'informació E.19- Fuga d'informació E.25- Pèrdua d'equips A.7- Ús no previst A.11- Accés no autoritzat A.12- Anàlisi de trànsit A.13- Repudi A.24- Denegació de servei A.25- Robatori A.26- Atac destructiu A.27- Ocupació enemiga A.29- Extorsió

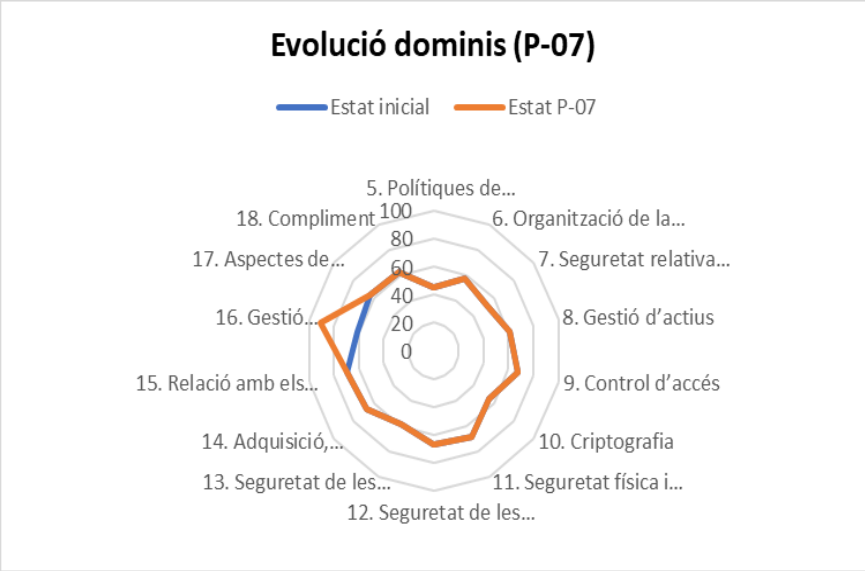
Diagrama radar	

Taula 18. Projecte de millora P-05

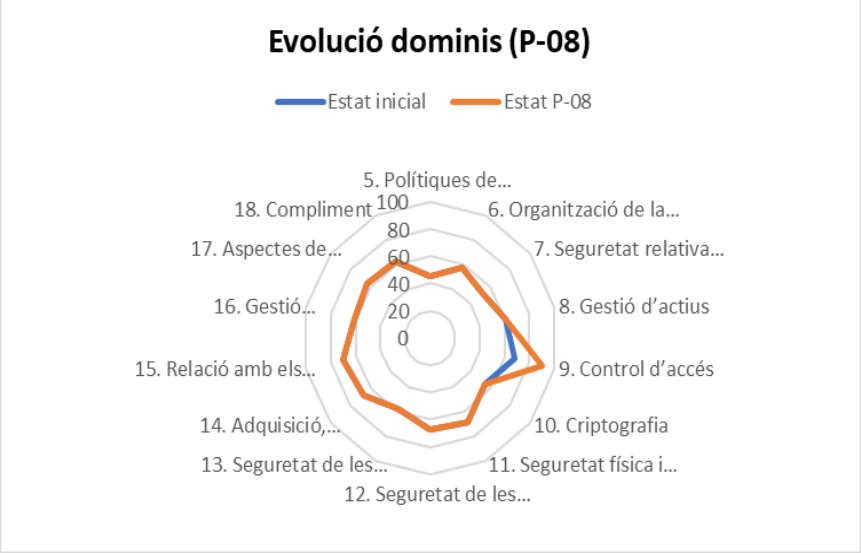
ID del projecte	P-06
Nom del projecte	Màquines trituradores de paper
Categoria	Seguretat física
Objectiu	Destruir la documentació confidencial, o amb informació sensible, de l'organització que es tengui en paper de tal manera que sigui impossible la seva reconstrucció
Responsabilitat	Departament de seguretat
Prioritat	Baixa
Planificació	Quick win
Dominis ISO	A.11 Seguretat física i de l'entorn
Cost	2.000 €
Riscos a mitigar	N.1- Foc N.2- Danys per aigua I.1- Foc I.2- Danys per aigua I.6- Tall de subministrament elèctric E.25- Pèrdua d'equips A.25- Robatori

Diagrama radar	

Taula 19. Projecte de millora P-06

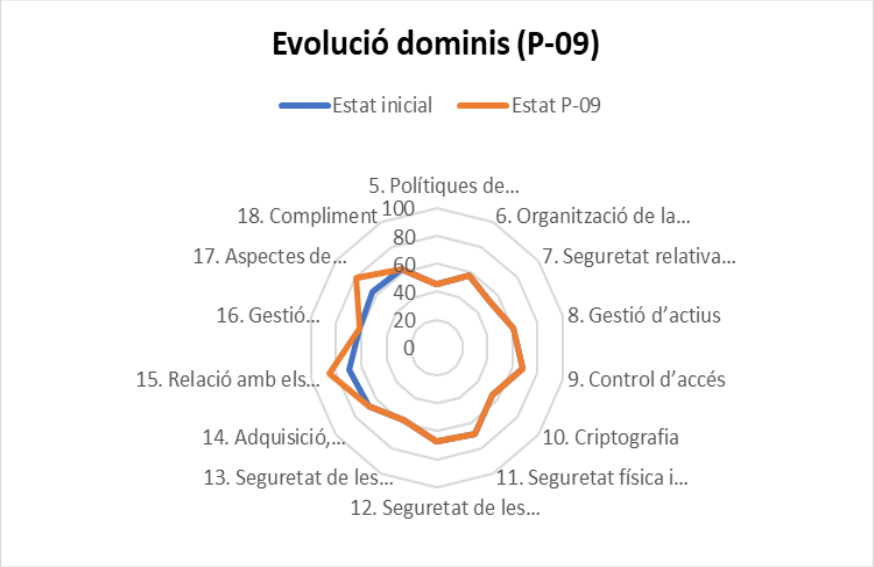
ID del projecte	P-07
Nom del projecte	Desplegament d'una solució per la protecció davant el malware dels servidors no protegits.
Categoria	Bastionat
Objectiu	Protegir els servidors contra el malware per tal d'evitar exposar els dispositius a algun dany
Responsabilitat	Departament de seguretat / IT
Prioritat	Alta
Planificació	Quick win
Dominis ISO	A.16 Gestió d'incidents de seguretat de la informació
Cost	12.000 €
Riscos a mitigar	E.8- Difusió de software maligne A.8- Difusió de software nociu
Diagrama radar	

Taula 20. Projecte de millora P-07

ID del projecte	P-08
Nom del projecte	Activació de l'autenticació de múltiples factors a l'Office 365 pels comptes d'usuari més crítiques i importants de l'organització
Categoria	Gestió d'accés
Objectiu	Els treballadors amb certs privilegis o responsabilitats dins de l'organització han d'iniciar sessió mitjançant múltiples maneres d'accés (contrasenya, token de seguretat o informació d'ADN)
Responsabilitat	Departament de seguretat / IT
Prioritat	Alta
Planificació	Quick win
Dominis ISO	A.09 Control d'accés
Cost	2.000 €
Riscos a mitigar	A.5- Suplantació de la identitat de l'usuari A.6- Abús de privilegi d'accés A.7- Ús no previst A.11- Accés no autoritzat A.15- Modificació deliberada de la informació
Diagrama radar	

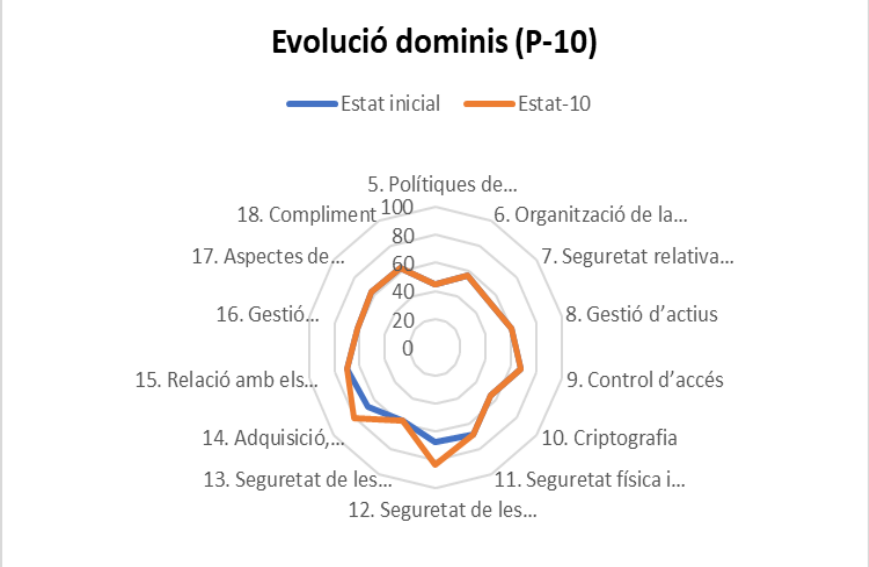
Taula 21. Projecte de millora P-08

ID del projecte	P-09
Nom del projecte	Definició d'un pla de continuïtat de negoci basat en un anàlisi d'impacte de negoci (BIA)
Categoria	Gestió de continuïtat
Objectiu	Identificar de manera clara els processos de cada entitat i analitzar el nivell d'impacte en relació amb la gestió del negoci
Responsabilitat	Departament de seguretat
Prioritat	Alta
Planificació	Curt termini
Dominis ISO	A.15 Relacions amb proveïdors A.17 Continuïtat de negoci
Cost	54.000 €

Riscos a mitigar	N.*-Desastre natural I.5- Averia d'origen físic o lògic I.6- Tall de subministrament elèctric I.8- Falla del servei de comunicacions E.1- Errors dels usuaris E.2- Errors de l'administrador E.4- Errors de configuració E.7- Deficiències en l'organització E.8- Difusió de software maligne E.15- Alteració accidental de la informació E.18- Destrucció d'informació E.19- Fuga d'informació E.24- Caiguda del sistema per esgotament de recursos A.6- Abús de privilegi d'accés A.8- Difusió de software nociu A.18- Destrucció de la informació A.19- Divulgació de la informació
Diagrama radar	

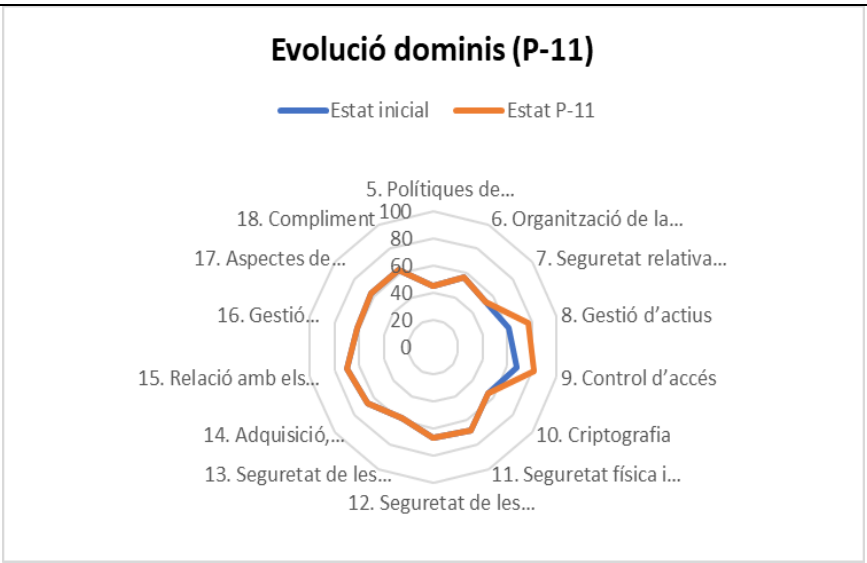
Taula 22. Projecte de millora P-09

ID del projecte	P-10
Nom del projecte	Implementació d'eines d'escaneig automatitzades de vulnerabilitats
Categoria	Bastionat
Objectiu	Facilitar la detecció de les vulnerabilitats dels sistemes
Responsabilitat	Departament de seguretat
Prioritat	Mitjana
Planificació	Curt termini
Dominis ISO	A.12 Seguretat de les operacions A.14 Adquisició, desenvolupament i manteniment de sistemes
Cost	25.000 €
Riscos a mitigar	I.7- Condicions inadequades de temperatura o humitat E.10- Errors de seqüència

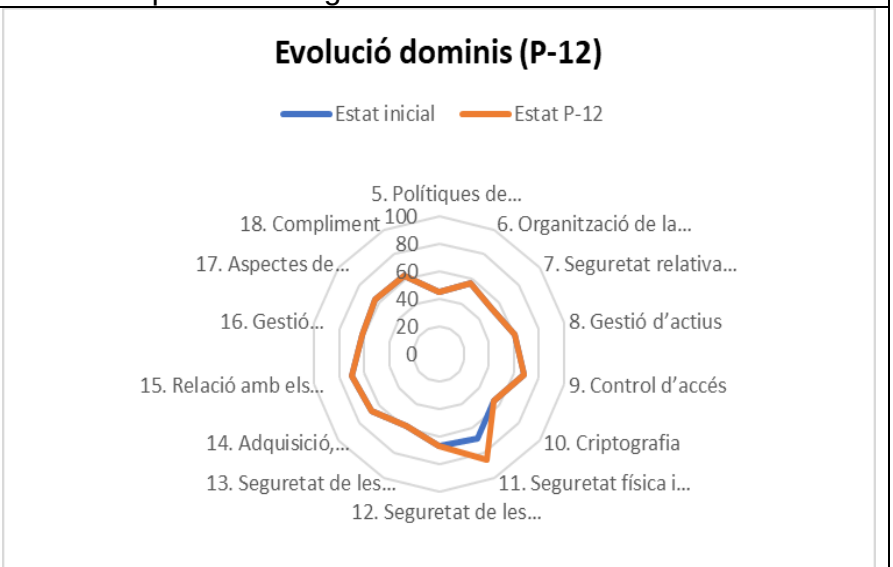
	E.20- Vulnerabilitats dels programes (software) A.10- Alteració de seqüència A.12- Anàlisi de trànsit A.22- Manipulació de programes A.23- Manipulació dels equips
Diagrama radar	

Taula 23. Projecte de millora P-10

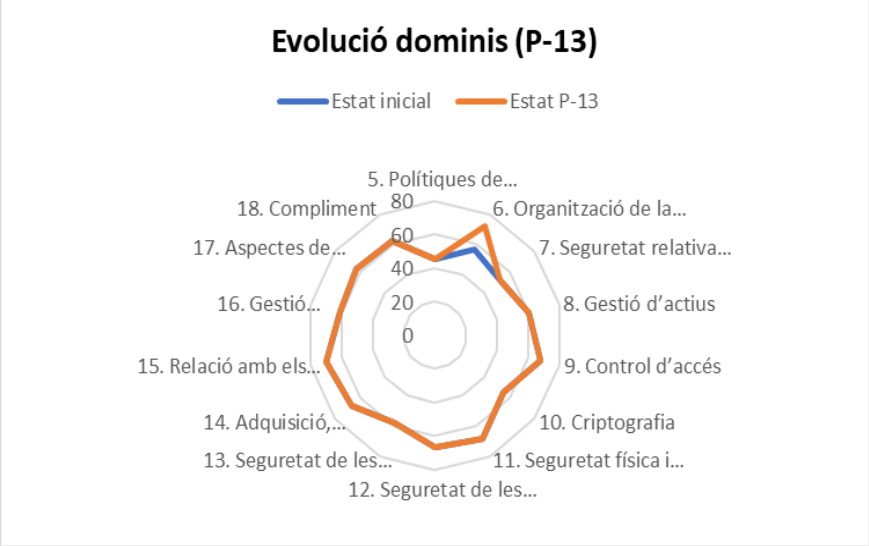
ID del projecte	P-11
Nom del projecte	Descobriment d'informació transmesa en els sistemes de l'organització relacionats amb el compliment de regulacions de seguretat aplicables
Categoria	Compliment
Objectiu	Revisió dels protocols de seguretat aplicats als accessos d'informació confidencial i restringida
Responsabilitat	Departament de seguretat
Prioritat	Mitjana
Planificació	Curt termini
Dominis ISO	A.08 Gestió d'actius A.09 Control d'accés
Cost	25.000 €
Riscos a mitigar	E.15- Alteració accidental de la informació E.18- Destrucció d'informació E.19- Fuga d'informació A.10- Alteració de seqüència A.15- Modificació deliberada de la informació A.18- Destrucció de la informació A.19- Divulgació de la informació

Diagrama radar	

Taula 24. Projecte de millora P-11

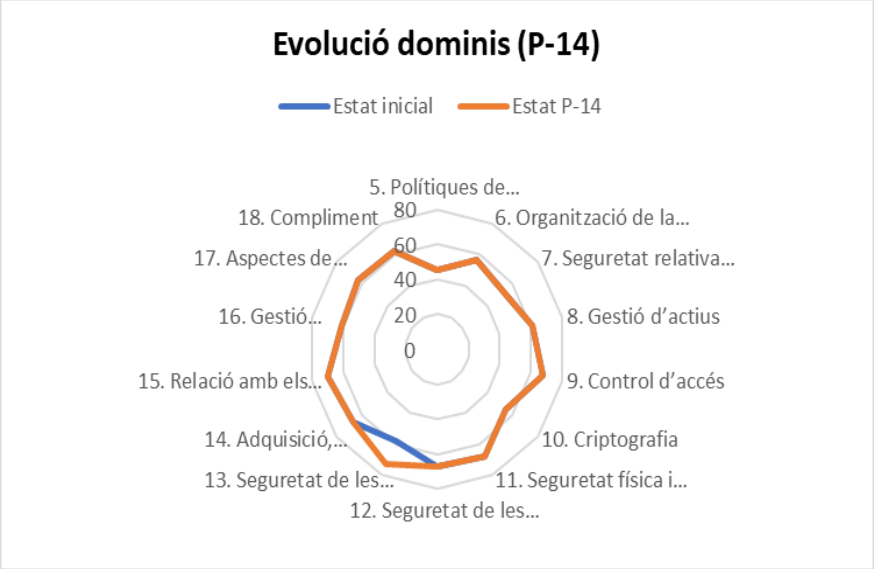
ID del projecte	P-12
Nom del projecte	Implementació de controls d'accés físic per accedir a les oficines centrals
Categoria	Seguretat física
Objectiu	Augmentar el control d'accés a les instal·lacions, mitjançant dispositius d'identificació única
Responsabilitat	Direcció
Prioritat	Mitjana
Planificació	Curt termini
Dominis ISO	A.11 Seguretat física i de l'entorn
Cost	20.000 €
Riscos a mitigar	A.5- Suplantació de la identitat de l'usuari A.7- Ús no previst A.11- Accés no autoritzat A.27- Ocupació enemiga
Diagrama radar	

Taula 25. Projecte de millora P-12

ID del projecte	P-13
Nom del projecte	Reforç dels recursos de l'equip de seguretat de l'organització
Categoria	Organització de la seguretat
Objectiu	Comptar amb més personal en l'equip de seguretat per tal d'oferir un major nivell de seguretat en l'organització i un control més exhaustiu de les polítiques de seguretat
Responsabilitat	Direcció
Prioritat	Alta
Planificació	Curt termini
Dominis ISO	A.6 Organització de la seguretat de la informació
Cost	110.000 €
Riscos a mitigar	E.7- Deficiències en l'organització E.24- Caiguda del sistema per esgotament de recursos E.28- Indisposició del personal A.28- Indisponibilitat del personal A.29- Extorsió A.30- Enginyeria social
Diagrama radar	

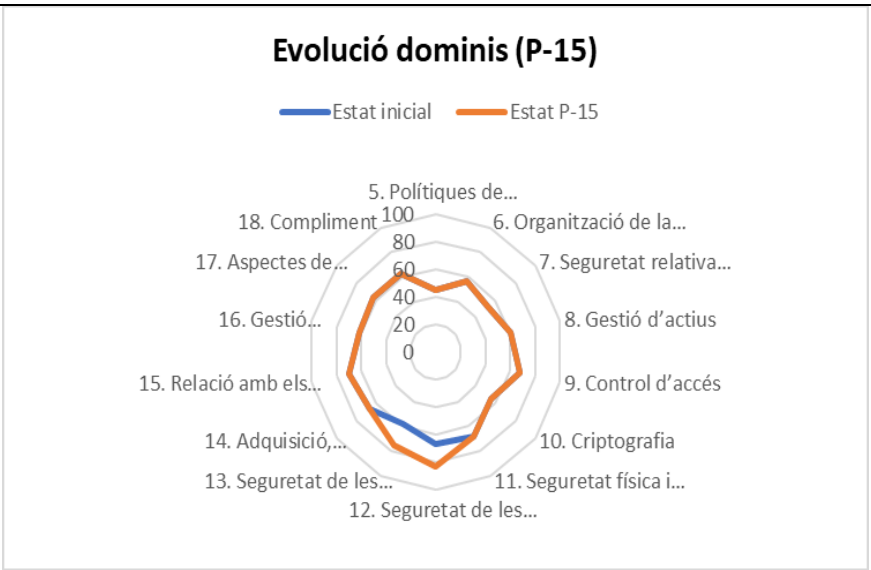
Taula 26. Projecte de millora P-13

ID del projecte	P-14
Nom del projecte	Monitorització de comunicacions de protocols insegurs
Categoria	Securització de les comunicacions
Objectiu	Revisar i identificar totes les comunicacions basades en protocols insegurs per tal d'establir-les en protocols segurs, per exemple, d'HTTP a HTTPS
Responsabilitat	IT
Prioritat	Alta
Planificació	Curt termini
Dominis ISO	A.13 Seguretat de les comunicacions
Cost	6.800 €
Riscos a mitigar	E.9- Errors de reencaminament E.10- Errors de seqüència

	A.9- Reencaminament de missatges A.12- Anàlisi de trànsit
Diagrama radar	

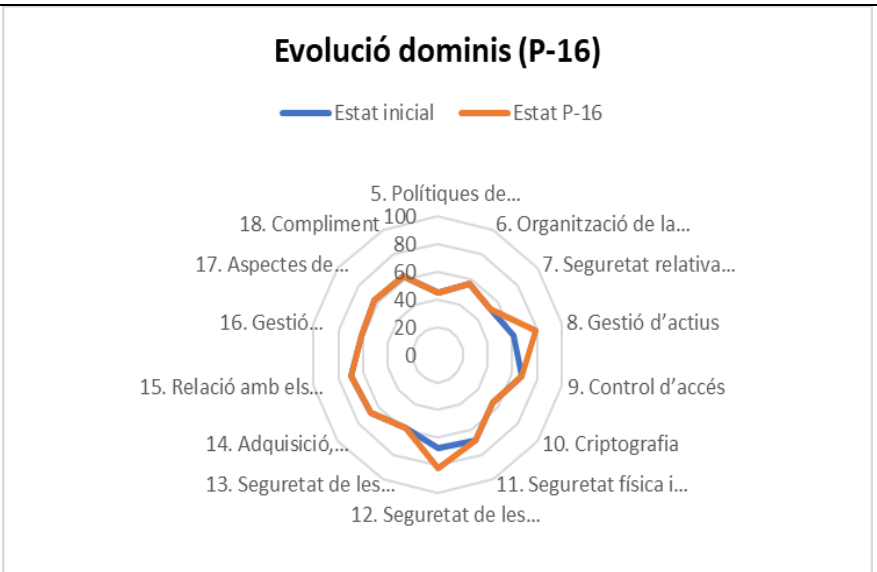
Taula 27. Projecte de millora P-14

ID del projecte	P-15
Nom del projecte	Implementació d'un servei de monitorització i resposta davant incidents de ciberseguretat
Categoria	Detecció i resposta d'incidents
Objectiu	Tenir un equip dedicat pel cas de patir un incident de ciberseguretat poder respondre a aquest amb major rapidesa i tenir una monitorització activa 24/7 per fer front a atacs de seguretat
Responsabilitat	Departament de seguretat
Prioritat	Alta
Planificació	Curt termini
Dominis ISO	A.12 Seguretat de les operacions A.13 Seguretat de les comunicacions
Cost	100.000 €
Riscos a mitigar	E.4- Errors de configuració E.8- Difusió de software maligne E.15- Alteració accidental de la informació E.21- Errors de manteniment/actualització de programes (software) E.23- Errors de manteniment/actualització d'equips (hardware) A.8- Difusió de software nociu A.10- Alteració de seqüència A.14- Intercepció de la informació (escolta) A.15- Modificació deliberada de la informació A.18- Destrucció de la informació A.22- Manipulació de programes A.23- Manipulació dels equips

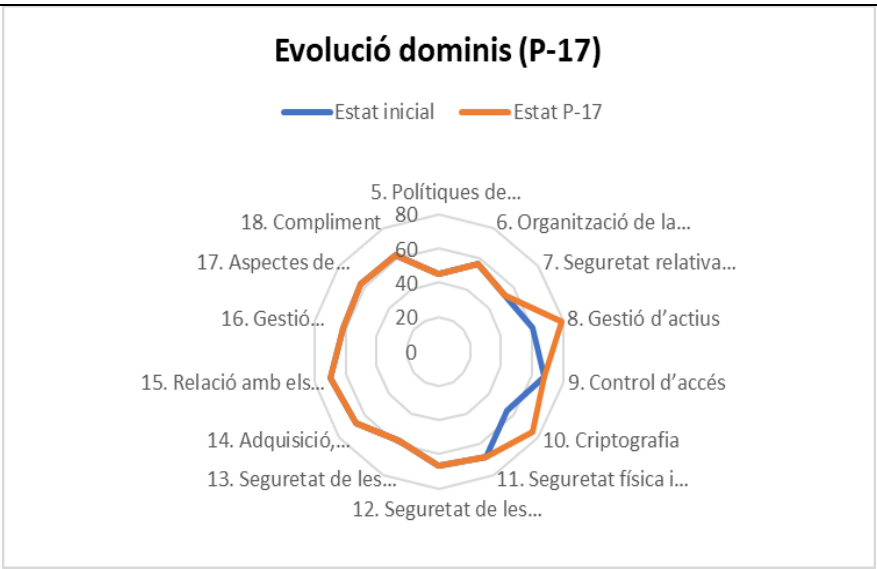
Diagrama radar	

Taula 28. Projecte de millora P-15

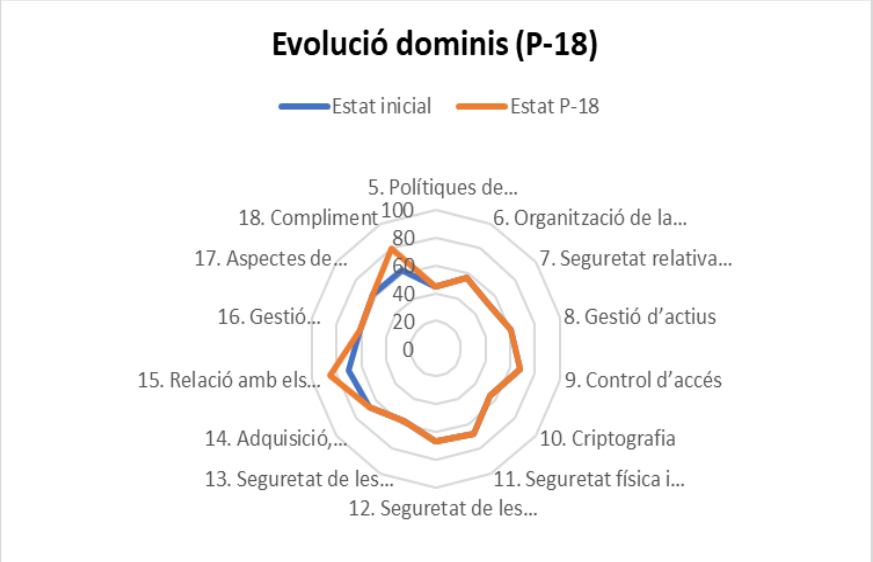
ID del projecte	P-16
Nom del projecte	Centralització i unificació de la gestió d'actius de la informació utilitzats per l'organització
Categoria	Securització
Objectiu	Mantenir i controlar els actius gestionant el treball, la planificació i la programació d'aquests per tal d'assegurar-se que els actius de l'organització es comptabilitzen, es despleguen, es mantenen, s'actualitzen i s'eliminen en el moment oportú
Responsabilitat	Departament de seguretat
Prioritat	Alta
Planificació	Curt termini
Dominis ISO	A.8 Gestió d'actius A.12 Seguretat de les operacions
Cost	13.200 €
Riscos a mitigar	E.15- Alteració accidental de la informació E.18- Destrucció d'informació E.19- Fuga d'informació E.21- Errors de manteniment/actualització de programes (software) E.23- Errors de manteniment/actualització d'equips (hardware) E.25- Pèrdua d'equips A.6- Abús de privilegi d'accés A.11- Accés no autoritzat

Diagrama radar	

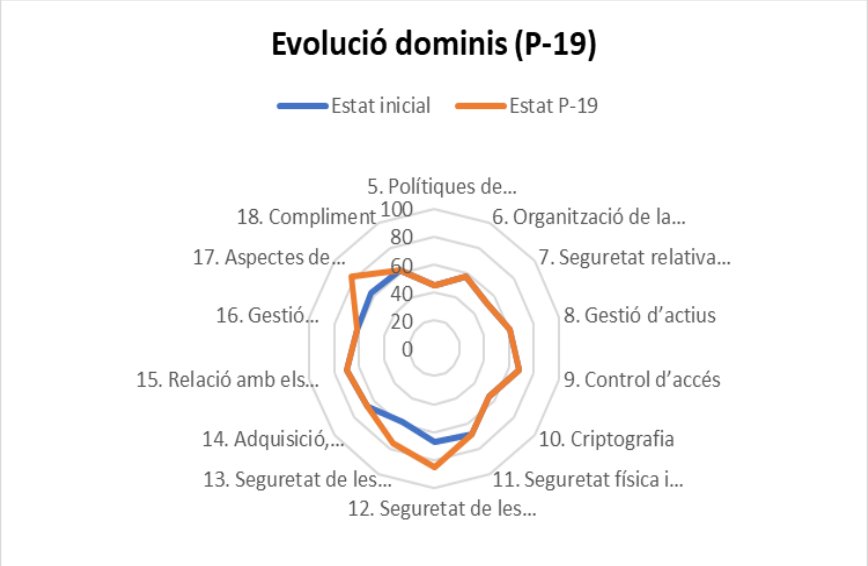
Taula 29. Projecte de millora P-16

ID del projecte	P-17
Nom del projecte	Definició d'un programa de prevenció de fuga d'informació
Categoria	Gestió d'accessos
Objectiu	Es pretén monitoritzar la xarxa de l'organització per evitar que es produeixin fugues d'informació
Responsabilitat	Departament de seguretat
Prioritat	Mitjana
Planificació	Mitjà termini
Dominis ISO	A.8 Gestió d'actius A.10 Criptografia
Cost	96.000 €
Riscos a mitigar	E.19- Fuga d'informació E.25- Pèrdua d'equips A.14- Intercepció de la informació (escolta) A.25- Robatori
Diagrama radar	

Taula 30. Projecte de millora P-17

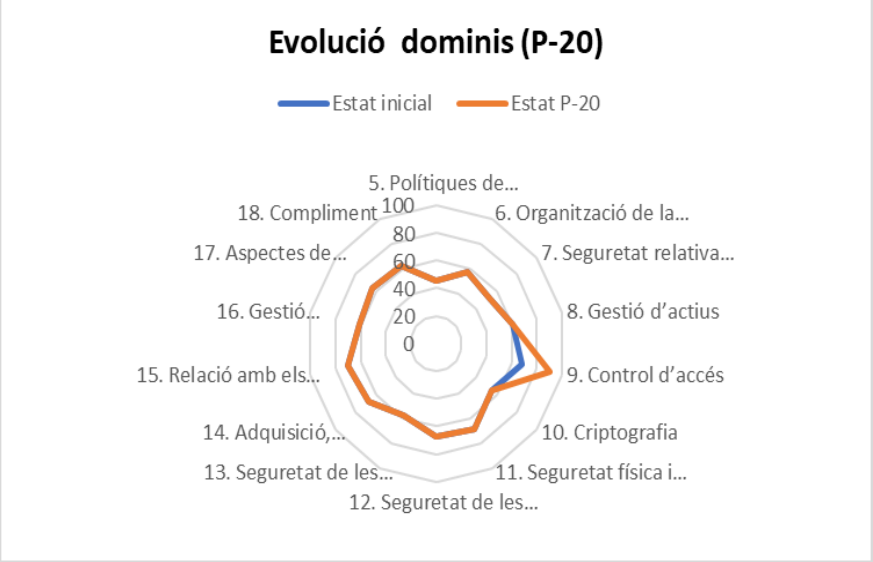
ID del projecte	P-18
Nom del projecte	Generació d'un cos normatiu pel compliment del marc de control intern de la seguretat de la informació
Categoria	Organització de seguretat
Objectiu	Tenir un conjunt definit de regles i normes per regular la implementació de les lleis i polítiques de l'organització
Responsabilitat	Departament de seguretat
Prioritat	Mitjana
Planificació	Mitjà termini
Dominis ISO	A.15 Relacions amb els proveïdors A.18 Compliment
Cost	33.000 €
Riscos a mitigar	E.2- Errors de l'administrador E.4- Errors de configuració E.7- Deficiències en l'organització E.9- Errors de reencaminament E.15- Alteració accidental de la informació E.18- Destrucció d'informació E.21- Errors de manteniment/actualització de programes (software) E.23- Errors de manteniment/actualització d'equips (hardware) E.24- Caiguda del sistema per esgotament de recursos A.7- Ús no previst A.9- Reencaminament de missatges A.11- Accés no autoritzat A.14- Intercepció de la informació (escolta) A.19- Divulgació de la informació A.22- Manipulació de programes A.23- Manipulació dels equips
Diagrama radar	

Taula 31. Projecte de millora P-18

ID del projecte	P-19
Nom del projecte	Protecció de totes les pàgines web corporatives
Categoria	Securització de comunicacions
Objectiu	Tenir les pàgines web de l'empresa protegides per evitar sofrir atacs de denegació de servei, fugues d'informació, atacs de tercers, etc.
Responsabilitat	Departament de seguretat / IT
Prioritat	Alta
Planificació	Mitjà termini
Dominis ISO	A.12 Seguretat en les operacions A.13 Seguretat en les comunicacions A.17 Continuïtat del negoci
Cost	25.000 €
Riscos a mitigar	A.6- Abús de privilegi d'accés A.7- Ús no previst A.9- Reencaminament de missatges A.10- Alteració de seqüència A.24- Denegació de servei A.26- Atac destructiu
Diagrama radar	

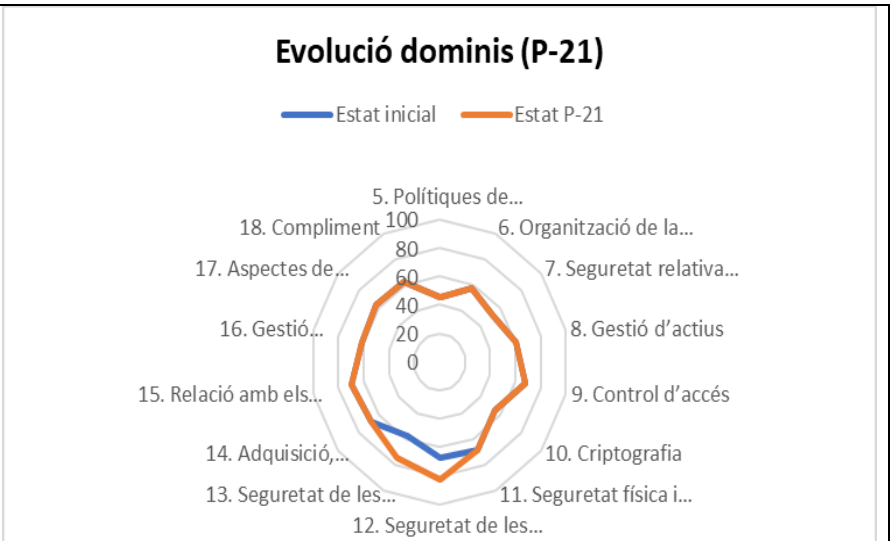
Taula 32. Projecte de millora P-19

ID del projecte	P-20
Nom del projecte	Millora del cicle de vida de les identitats de l'organització
Categoria	Gestió d'accessos
Objectiu	Millorar els processos d'identificació del registre de treballadors i la verificació de la seva identitat, tenguent en compte els permisos i els privilegis per accedir als recursos i el procés d'autenticació
Responsabilitat	Departament de seguretat
Prioritat	Alta
Planificació	Mitjà termini

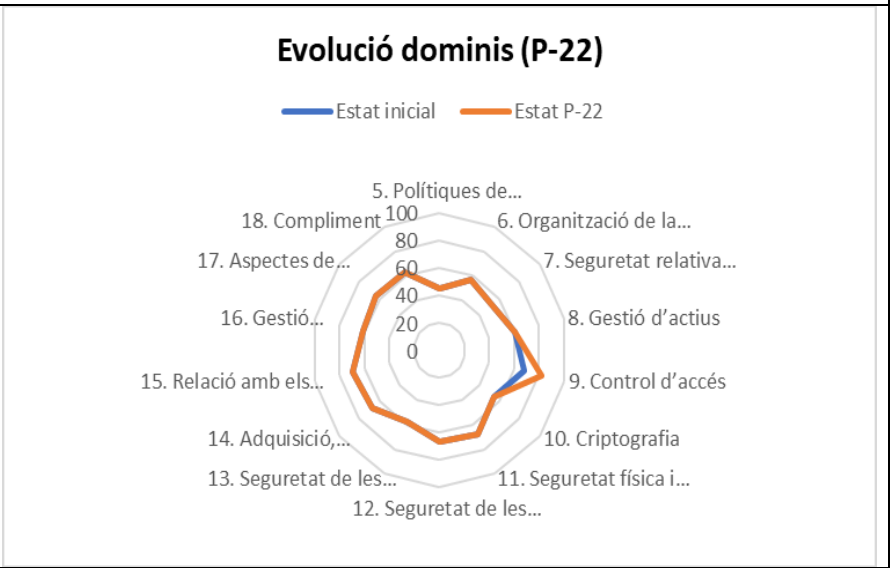
Dominis ISO	A.9 Control d'accés
Cost	122.000 €
Riscos a mitigar	A.5- Suplantació de la identitat de l'usuari A.6- Abús de privilegi d'accés A.11- Accés no autoritzat
Diagrama radar	

Taula 33. Projecte de millora P-20

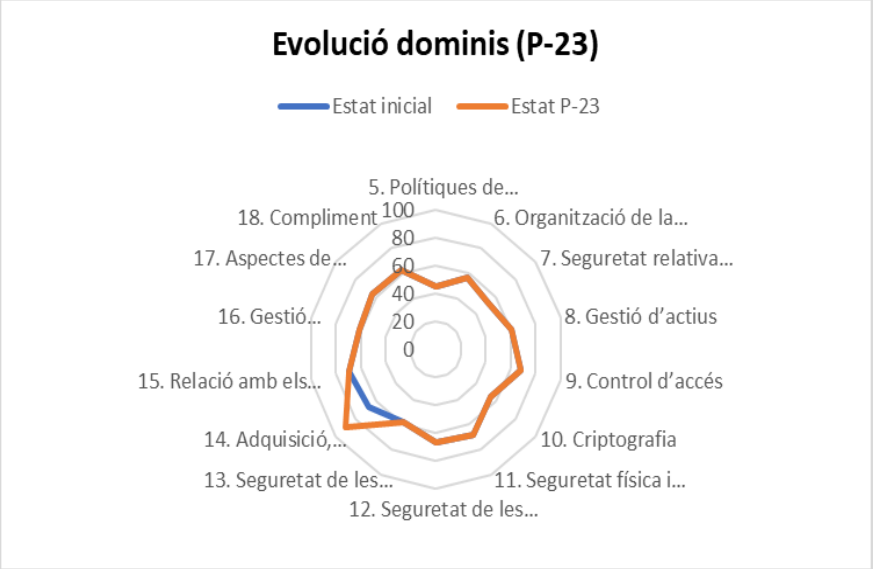
ID del projecte	P-21
Nom del projecte	Implementar una eina pel govern dels distints clouds gestionats per l'organització
Categoria	Gestió d'accessos
Objectiu	Simplificar i accelerar les transaccions, alhora que es manté el control sobre els riscos, el cost dels actius i el compliment normatiu
Responsabilitat	Departament de seguretat / IT
Prioritat	Alta
Planificació	Mitjà termini
Dominis ISO	A.12 Seguretat en les operacions A.13 Seguretat en les comunicacions
Cost	76.000 €
Riscos a mitigar	E.2- Errors de l'administrador E.24- Caiguda del sistema per esgotament de recursos

Diagrama radar	

Taula 34. Projecte de millora P-21

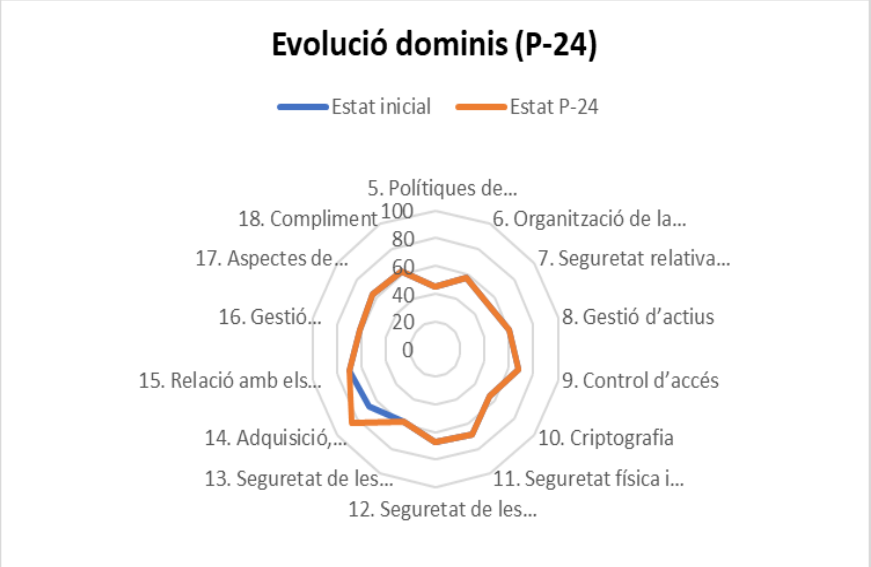
ID del projecte	P-22
Nom del projecte	Implementar una eina per protegir les contrasenyes dels usuaris administradors
Categoria	Gestió d'accessos
Objectiu	Protegir les contrasenyes dels administradors mitjançant un gestor de contrasenyes per tal d'evitar que aquestes siguin revelades i utilitzades per personal no autoritzat
Responsabilitat	Departament de seguretat
Prioritat	Mitjana
Planificació	Mitjà termini
Dominis ISO	A.9 Control d'accés
Cost	112.000 €
Riscos a mitigar	A.5- Suplantació de la identitat de l'usuari A.6- Abús de privilegi d'accés A.11- Accés no autoritzat
Diagrama radar	

Taula 35. Projecte de millora P-22

ID del projecte	P-23
Nom del projecte	Implementació d'una metodologia de desenvolupament segur de sistemes i/o aplicacions
Categoria	Desenvolupament i manteniment d'aplicacions
Objectiu	Disposar d'un model basat en la realització de comprovacions de seguretat contínues durant tot el cicle de vida del sistema i/o l'aplicació
Responsabilitat	Departament de seguretat / IT
Prioritat	Alta
Planificació	Llarg termini
Dominis ISO	A.14 Adquisició, desenvolupament i manteniment de sistemes
Cost	58.800 €
Riscos a mitigar	E.2- Errors de l'administrador E.4- Errors de configuració E.8- Difusió de software maligne E.20- Vulnerabilitats dels programes (software) E.21- Errors de manteniment/actualització de programes (software) A.8- Difusió de software nociu A.22- Manipulació de programes
Diagrama radar	

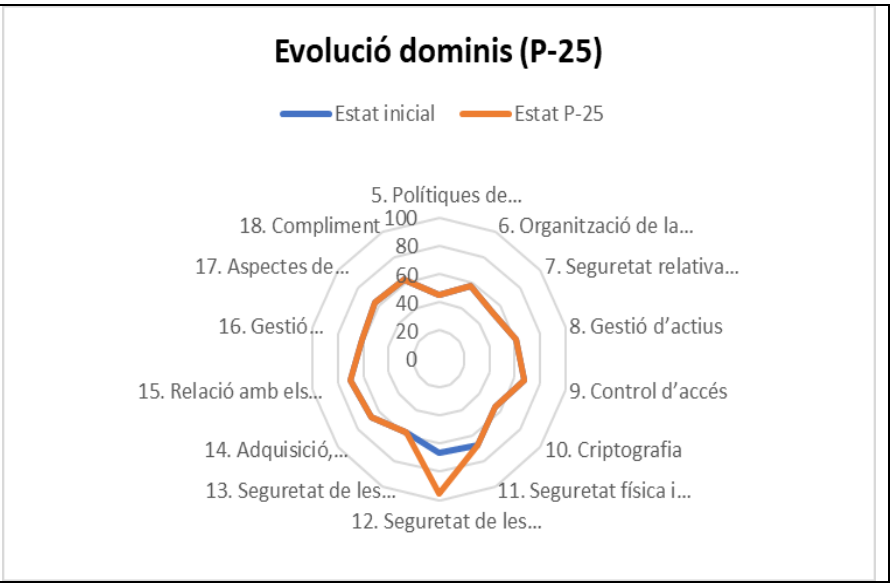
Taula 36. Projecte de millora P-23

ID del projecte	P-24
Nom del projecte	Implementar una eina per l'auditoria de seguretat de codi font
Categoria	Desenvolupament i manteniment d'aplicacions
Objectiu	Revisar constantment el codi font per tal de detectar possibles errors en pràctiques de programació insegures de manera automàtica
Responsabilitat	Departament de seguretat / IT
Prioritat	Mitja
Planificació	Mitjà termini

Dominis ISO	A.14 Adquisició, desenvolupament i manteniment de sistemes
Cost	82.000 €
Riscos a mitigar	E.4- Errors de configuració E.15- Alteració accidental de la informació E.18- Destrucció d'informació A.19- Divulgació de la informació
Diagrama radar	

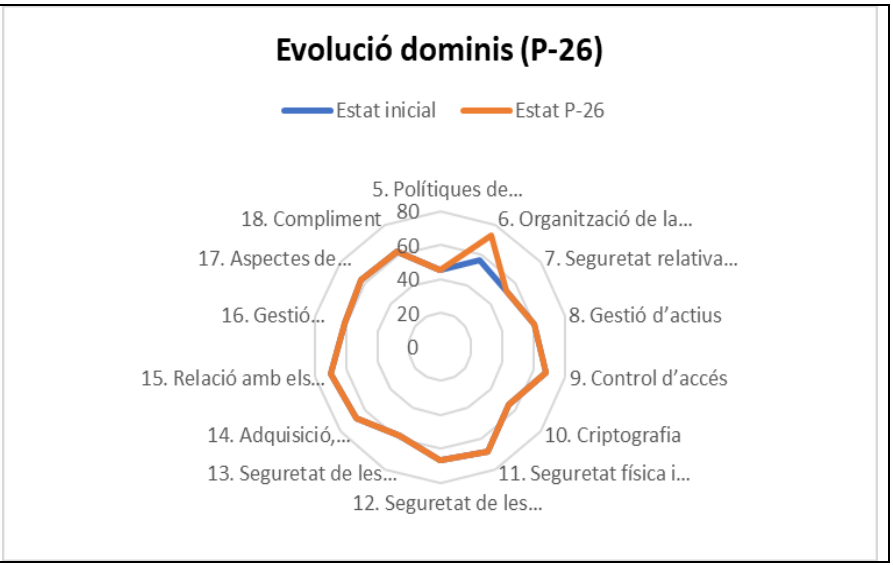
Taula 37. Projecte de millora P-24

ID del projecte	P-25
Nom del projecte	Monitorització de pàgines web fraudulentes i deep web per detectar filtracions d'informació de l'organització
Categoria	Detecció i resposta a incidents
Objectiu	Monitoritzar pàgines web fraudulentes i la deep web per verificar que no hi hagi informació exposada de la companyia
Responsabilitat	Departament de seguretat / IT
Prioritat	Mitja
Planificació	Llarg termini
Dominis ISO	A.12 Seguretat en les operacions
Cost	25.000 €
Riscos a mitigar	E.19- Fuga d'informació A.5- Suplantació de la identitat de l'usuari A.14- Intercepció de la informació (escolta) A.24- Denegació de servei A.26- Atac destructiu

Diagrama radar	

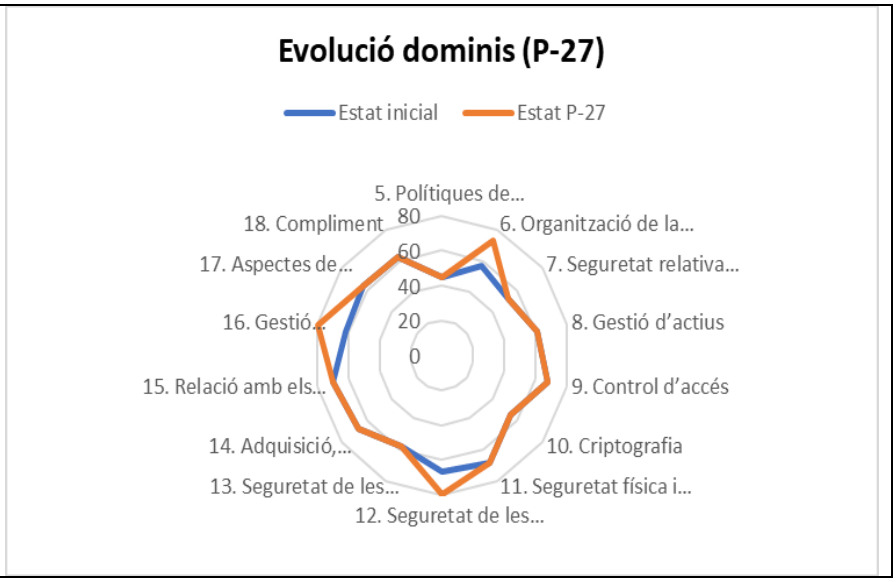
Taula 38. Projecte de millora P-25

ID del projecte	P-26
Nom del projecte	Implementació d'una metodologia de gestió de riscos enfocada a ciberamenaces critiques per l'organització
Categoria	Organització de seguretat
Objectiu	Tenir estipulada la caracterització del sistema, la identificació d'amenaces i vulnerabilitats, el control d'anàlisi, la determinació del risc, l'anàlisi de l'impacte, les recomanacions de control i el resultat de la implementació juntament amb el pla d'acció
Responsabilitat	Departament de seguretat
Prioritat	Baixa
Planificació	Llarg termini
Dominis ISO	A.6 Organització de la seguretat de la informació
Cost	35.000 €
Riscos a mitigar	E.8- Difusió de software maligne E.20- Vulnerabilitats dels programes (software) A.10- Alteració de seqüència A.15- Modificació deliberada de la informació A.18- Destrucció de la informació A.19- Divulgació de la informació A.24- Denegació de servei

Diagrama radar	

Taula 39. Projecte de millora P-26

ID del projecte	P-27
Nom del projecte	Definició de procediments davant distintes casuístiques a seguir davant la resposta a incidents de ciberseguretat
Categoria	Organització de seguretat
Objectiu	Tenir definit un conjunt de processos, requisits i controls per administrar adequadament els riscos i les amenaces que poden afectar a l'organització en cas de sofrir un incident de ciberseguretat
Responsabilitat	Departament de seguretat
Prioritat	Mitjana
Planificació	Llarg termini
Dominis ISO	A.6 Organització de la seguretat de la informació A.12 Seguretat en les operacions A.16 Gestió d'incidents de la seguretat de la informació
Cost	27.000 €
Riscos a mitigar	E.8- Difusió de software maligne E.20- Vulnerabilitats dels programes (software) A.10- Alteració de seqüència A.15- Modificació deliberada de la informació A.18- Destrucció de la informació A.19- Divulgació de la informació A.24- Denegació de servei

Diagrama radar	

Taula 40. Projecte de millora P-27

6. Auditoria de compliment de la ISO/IEC 27002:2013

A n'aquest punt del projecte ja coneixem els actius de l'empresa i hem avaluat les amenaces d'aquests a l'anàlisi de riscos, com hem pogut veure anteriorment. A partir d'aquesta anàlisi hem pogut definir projectes de millora per tal de millorar l'estat de la seguretat de l'organització.

Per tal d'analitzar i avaluar fins a quin punt l'empresa compleix amb les bones pràctiques en matèria de seguretat ens basarem en el marc de control de l'estat de la seguretat, la ISO/IEC 270002:2013.

6.1. Metodologia

Per tal de mesurar el nivell de maduresa de la seguretat, s'analitzaran els controls o les mesures preventives sobre bones pràctiques per a la gestió de la seguretat de la informació, que estan organitzats en 113 controls, 14 àrees i 35 objectius de control. A més, hi ha diferents aspectes als quals les mesures preventives actuen reduint el risc i, per tant, millorant la seguretat dins de l'organització, com per exemple:

- Formació de les pràctiques mitjançant documents escrits o aprovats.
- Política de personal.
- Sol·licituds tècniques (software, hardware o comunicacions).
- Seguretat física.

Per desenvolupar l'auditoria de compliment utilitzarem el Model de Maduresa de Capacitat (CMM), el qual ja hem citat anteriorment al capítol 2 "Contextualització i documentació", on per avaluar cada control ens basarem en l'escala d'estat de maduresa dels controls establerts per la normativa, Taula 1.

6.2. Avaluació de la maduresa

A continuació tornarem a valorar els controls de maduresa del sistema. Per avaluar la maduresa de la seguretat utilitzarem els criteris definits a la Taula 1 del Model de Maduresa de Capacitat (CMM) pels distints controls de la norma ISO/IEC 27002:2013. [6]

A l'Annex 8 trobarem dues taules amb els requisits generals i els controls de la norma, juntament amb la valoració d'aquests en el seu estat inicial, estat final i l'estat desitjable seguint el CMM. També hi trobarem els resultats representats en forma de gràfiques, la qual cosa ens permetrà veure l'evolució de manera visual, entre l'estat inicial i l'estat final, i l'estat desitjable i l'estat final que s'ha aconseguit.

6.3. Presentació dels resultats

Finalment, presentarem els resultats obtinguts seguint el format de l'informe d'auditoria de l'organització, consultar Annex 9.

7. Conclusions

En la creació del Pla Director de Seguretat es pretenia protegir els processos de negoci de l'organització durant les vint-i-quatre hores i els set dies de la setmana, els quals són: el procés de venda, la informació dels clients, la informació confidencial de l'empresa i el software de la gestió hotelera. Per establir les bases del PDS per tal d'implementar un Sistema de Gestió de la Seguretat de la Informació des del seu inici, cal realitzar una anàlisi de la situació actual, definir la política de seguretat de l'empresa, revisar la gestió de rols i responsabilitats, elaborar una anàlisi de riscos juntament amb la declaració d'aplicabilitat, realitzar un inventari d'actius de l'organització, analitzar les possibles amenaces i el seu impacte i probabilitat, descriure propostes de projectes de millora i finalment amb tota aquesta informació, realitzar l'auditoria de compliment de la ISO/IEC 27001:2013. Per aconseguir-ho, s'ha comptat amb personal extern i expert en la matèria de Seguretat de la Informació juntament amb el personal propi de l'organització. Els projectes que es generin a conseqüència d'aquesta implementació, seran dirigits pel personal intern de l'empresa, concretament pel departament de seguretat sota la supervisió del seu responsable.

És important tenir en compte que dins de qualsevol organització la implementació del SGSI no ha de quedar-se només en fer l'anàlisi inicial i la implementació de millores en un moment puntual, sinó que és essencial fer un seguiment continu i constant en la millora de la seguretat al llarg del temps per tal de millorar totalment els processos de l'organització.

Un cop finalitzat aquest projecte, som més conscients de l'estat en què es troba l'organització i del nivell de compliment de la Seguretat de la Informació. D'aquesta manera, malgrat que no es cobreixin tots els controls amb el nivell desitjat per l'organització, ja que s'han detectat múltiples carències no rellevants relacionades amb les mesures de seguretat i les polítiques de la pròpia organització, el desenvolupament dels projectes proposats ha suposat una considerable millora del sistema en termes de maduresa de la Seguretat de la Informació.

Per tal d'aconseguir finalitzar el TFM dins del termini establert ha estat essencial seguir amb la planificació que se'ns va proposar, la qual estava estructurada en sis fases, on en cadascuna d'elles hem lliurat els entregables associats a cada una de les fases. Personalment, he aconseguit lliurar totes i cadascuna de les entregues dins de la data prevista, però no ha estat una tasca senzilla, sinó ben bé el contrari, ja que ha suposat invertir una gran quantitat d'hores en la investigació de termes que desconeixia, esbrinar com s'havia d'estructurar la documentació i en la realització d'aquesta en si. En general, puc afirmar que no he hagut d'introduir canvis per garantir l'èxit del treball perquè seguint la planificació juntament amb l'esforç personal i les facilitats que he rebut per part de l'organització en qüestió, he pogut arribar amb èxit al final del treball.

Respecte a les línies de futur queden pendents aquelles millores esmentades a l'informe d'auditoria per tal de millorar el sistema. A més també formen part de les línies de futur aquells controls que no han avançat perquè el pressupost ha estat insuficient. Es remarca que és necessari sol·licitar més recursos, tant econòmics com de personal, per poder fer front a aquestes mancances.

Vivim en una era digital on cada dia esdevenen atacs informàtics arreu del món. Sovint ens trobam en notícies sobre empreses o entitats en l'àmbit del turisme que han patit incidents de seguretat, el que posa de manifest, una vegada més, que cal ser conscients dels riscos que suposa per a la continuïtat del negoci.

8. Glossari

Actiu: informació o element relacionat amb el tractament de la mateixa (sistemes, suports, edificis, persones...) que tingui valor per a l'organització.

Amenaça: acció o esdeveniment negatiu facilitat per una vulnerabilitat que té com a resultat un impacte no desitjat en un sistema o aplicació.

Contrasenya: cadena de caràcters que s'ha de proporcionar per obtenir l'autorització per accedir a un inici de sessió d'un sistema o recurs.

Control d'accés: mecanisme que gestiona l'accés a dades o recursos en funció de la identificació prèviament autenticada

CMM (Model de Maduresa de Capacitats): model del SEI (Software Engineering Institute) que les organitzacions poden utilitzar per determinar les seves capacitats per desenvolupar o mantenir software, basat en un procés de millora contínua a l'organització.

CPD (Centre de Processament de Dades): instal·lació que centralitza les operacions i la infraestructura de TI de l'organització, on s'emmagatzemen, es processen, es tracten i es difonen dades i aplicacions.

ISO (International Organization for Standardization): organització no governamental que es compon per diferents representants d'organismes de normalització els quals es dediquen a la creació de normes o estàndards per assegurar la qualitat, la seguretat i l'eficiència dels productes i serveis.

MAGERIT (Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes d'Informació): metodologia d'anàlisi i gestió elaborada per minimitzar els riscos d'implementació i l'ús de les TI, enfocada a l'administració pública.

PDCA: cicle de Deming, basat en quatre fases essencials, Plan, Do, Check i Act, que tota empresa ha de dur a terme de manera sistemàtica per aconseguir la millora contínua de la qualitat.

PDS (Pla Director de Seguretat): definició i priorització d'un conjunt de projectes en matèria de seguretat de la informació amb l'objectiu de reduir els riscos als quals està exposada l'organització fins a uns nivells acceptables.

Privacitat: control que exerceix un usuari sobre la seva informació per tal de limitar la quantitat de persones autoritzades a obtenir-la.

Risc: amenaça que pot atemptar contra la seguretat dels nostres recursos o informació.

SGSI (Sistema de Gestió de la Informació): guia que permet a les empreses avaluar els riscos i definir les aplicacions de control per poder eliminar-los o minimitzar-ne les conseqüències negatives.

TI (Tecnologia de la Informació): tecnologies de la informació i la comunicació que s'encarreguen de la gestió de la informació de l'empresa, relacionat amb internet.

TFM (Treball de Fi de Màster): projecte que realitza l'alumne, sota la supervisió del seu tutor, on demostra i aplica els coneixements adquirits durant el màster cursat.

Usuari: persona o procés autoritzat per accedir als recursos dels sistemes d'informació.

9. Bibliografia

[1] Plan director de Seguridad, INCIBE, https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf, 21.02.2022

[2] Guía de indicadores de gestión para la seguridad de la información, MINTIC

[3] Guía de gestión de riesgos, MINTIC

[4] Controles de Seguridad y privacidad de la información, MINTIC

[5] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Informacion, ENS, Madrid, 2012

[6] Norma Española UNE-EN ISO/IEC 27001, UNE, Mayo 2017

[7] Norma Española UNE-EN ISO/IEC 27002, UNE, Mayo 2017

Apunts de l'assignatura de Sistemes de Gestió de Seguretat de la Informació (M1.709).

Apunts de l'assignatura Auditoria tècnica (M1.710).

Coneixements aportats pel tutor.

10. Annexos

10.1. Annex 1 – Política de seguretat.

- **Àmbit d'aplicació**.

El contingut d'aquesta política ha de ser conegut i és d'obligat compliment per a tot el personal, tant intern com extern, que tingui accés als sistemes d'informació de l'empresa o a les dades sota la seva responsabilitat.

Aquest manual és aplicable a tots els recursos informàtics propietat de l'empresa en qüestió, considerant com a recursos informàtics:

- Xarxes corporatives i recursos compartits de xarxa.
- Aplicacions informàtiques d'escriptori o executades remotament.
- Accés a Internet.
- Serveis de correu electrònic.
- Serveis de missatgeria, trucades de veu i vídeo per Internet.
- Estacions de treball.
- Ordinadors portàtils, tauletes i telèfons mòbils.
- Suports d'emmagatzematge (discos externs, memòries USB, CD/DVD, cintes magnètiques, emmagatzematge en el núvol, etc.).
- I qualsevol altre dispositiu tecnològic o servei informàtic proporcionat per l'empresa per al normal exercici de les tasques professionals dels empleats.

Es garantirà la seguretat de la informació al llarg de totes les fases del seu cicle de vida, incloent-hi la seva generació, distribució, magatzematge, processament, transport, consulta i destrucció, així com als sistemes que els suporten, des de la seva anàlisi, disseny, desenvolupament, implantació, explotació, integració i manteniment.

- **Termes i definicions.**

  - Nom de l'empresa: Totes les societats compreses en el grup d'empreses a tot el món. Tret que s'estableixi una altra cosa, les expressions "empresa", "societat", "organització" o "companyia", s'entenen referides a totes i cadascuna de les societats en el grup d'empreses.

  - Personal o empleats: Tots els consellers, directius i altres empleats de l'empresa, independentment de la seva forma de contractació, quan actuïn en la seva condició de tals, és a dir, en nom i per compte de l'empresa, i tant si ho fan directa com indirectament, per si o a través de persona interposada o per mitjà d'alguna societat o un altre tipus d'entitat controlada.

- Tercers. Els proveïdors de béns i serveis de l'empresa que mantinguin relacions comercials amb l'empresa.

- SGSI: Són les sigles del Sistema de Gestió de la Seguretat de la Informació (regulat per la Norma UNE-ISO/IEC 27001), que és un conjunt d'elements interrelacionats o interactuats (estructura organitzativa, polítiques, planificació d'activitats, responsabilitats, processos, procediments i recursos) que utilitza una organització per a establir una política i uns objectius de seguretat de la informació i aconseguir aquests objectius, basant-se en un enfocament de gestió del risc i de millora contínua.

- Part interessada: Persona o grup que té un interès en l'acompliment o èxit de l'organització.

- Autenticitat: Propietat que una persona i/o empresa que ha accedit i utilitzat la informació és el que afirma ser.

- Confidencialitat: Propietat de la informació de no posar-se a disposició o ser revelades a persones i/o empreses no autoritzades.

- Integritat: Propietat o característica consistent on l'actiu d'informació no ha estat alterat de manera no autoritzada.

- Traçabilitat: Qualitat que permet que totes les accions realitzades sobre la informació o un sistema de tractament de la informació siguin associades de manera inequívoca a una persona i o empresa.

- Disponibilitat: Propietat de la informació d'estar accessible i utilitzable en el moment que es requereixi per la persona i o empresa autoritzada.

- Actiu: En relació amb la seguretat de la informació, es refereix a qualsevol informació o element relacionat amb el tractament de la mateixa (sistemes, suports, edificis, persones...) que tingui valor per a l'organització.

- Risc: Possibilitat que una amenaça concreta pugui explotar una vulnerabilitat per a causar una pèrdua o mal en un actiu d'informació. Sol considerar-se com una combinació de la probabilitat d'un esdeveniment i les seves conseqüències.

- Amenaça: Causa potencial d'un incident no desitjat, que pot provocar danys a un sistema o a l'organització.

- Anàlisi de riscos: Procés per a comprendre la naturalesa del risc i determinar el nivell de risc.

- Tractament de riscos: Procés de modificar el risc, mitjançant la implementació de controls.

- **Lideratge i compromís de la direcció.**

La direcció de l'empresa es compromet a facilitar i proporcionar els recursos necessaris per a l'establiment, implantació, manteniment i millora del SGSI de l'entitat, així com a demostrar lideratge i compromís respecte a aquest, a través de la constitució del Comitè de Seguretat de la Informació que tindrà la responsabilitat de:

- Assegurar l'establiment de la present política i els objectius de la seguretat de la informació, i que aquests siguin compatibles amb l'estratègia de negoci de l'empresa.

- Assegurar la integració i el compliment dels requisits aplicables del SGSI en els processos de l'entitat.

- Assegurar que els recursos necessaris per al SGSI estiguin disponibles.

- Comunicar la importància d'una gestió de la seguretat eficaç i conforme amb els requisits del SGSI.

- Assegurar que el SGSI aconsegueix els resultats previstos.

- Dirigir i fer costat a les persones per a contribuir a l'eficàcia del SGSI.

- Promoure la millora contínua.

- Donar suport a altres rols pertinents de la direcció, liderant a les seves àrees de responsabilitat en seguretat de la informació.

El detall de les funcions específiques del Comitè Seguretat de la Informació, es descriuran en la Normativa d'Organització de la Seguretat de la Informació.

- **Funcions i/o responsabilitats de la seguretat de la informació.**

L'aplicació i compliment de la present política és responsabilitat de tots els empleats, i tercers de l'empresa, independentment de qui sigui el responsable d'aquests tractaments.

En conseqüència, tots els empleats i aquells tercers subcontractats, són copartícips d'aquesta responsabilitat, havent de treballar, des de la posició que ocupin i independentment de la responsabilitat que explícitament se'ls assigni, cap a la consecució d'una adequada protecció de la informació.
Els empleats de l'empresa, així com el personal subcontractat o col·laboradors externs, hauran de conèixer, assumir i complir la política, normatives i

procediments de seguretat, estant obligats a mantenir el secret professional i la confidencialitat de les dades manejades en el seu entorn laboral i havent de comunicar, amb caràcter d'urgència i segons els procediments establerts, les possibles incidències o problemes que es detectin.

L'incompliment manifest de les normes de seguretat de la informació podrà implicar l'inici de les mesures disciplinàries oportunes i, si és elmcas, les responsabilitats legals corresponents.

- **Revisió de la política de seguretat de la informació.**

El Sistema de Gestió de Seguretat de la Informació (SGSI) es mantindrà permanentment actualitzat i es revisarà de manera periòdica, per a garantir la seva adequació a les necessitats específiques de l'empresa. En aquest procés s'implicaran des d'un principi als membres de l'organització, promovent una actitud positiva, crítica i constructiva en permanent cerca de la millora i la qualitat en el tractament de la informació.

DESENVOLUPAMENT DE LA POLÍTICA

- **Organització de la seguretat.**

L'objectiu del present domini és establir les directrius per a l'administració de la seguretat de la informació, com a part fonamental dels objectius i activitats de l'organització.

Per a això, es definirà formalment un àmbit de gestió per a efectuar tasques com ara l'aprovació de les polítiques de seguretat, la coordinació de la implementació de la seguretat i l'assignació de funcions i responsabilitats.
Per a una actualització adequada en matèria de seguretat es contemplarà la necessitat de disposar de fonts amb coneixement i experimentades per a l'assessorament, cooperació i col·laboració en matèria de seguretat de la informació.

- **Seguretat lligada als recursos humans.**

L'objectiu del present domini és la necessitat d'educar i informar el personal des del seu ingrés i en forma contínua, qualsevol sigui la seva situació d'activitat, sobre les mesures de seguretat que afecten el desenvolupament de les seves funcions i de les expectatives dipositades en ells en matèria de seguretat i assumptes de confidencialitat.

És necessari reduir els riscos d'error humà, comissió d'actes il·lícits, ús inadequat d'instal·lacions i recursos i maneig no autoritzat de la informació, al costat de la definició de possibles sancions que s'aplicaran en cas d'incompliment.

Es requereix explicitar les responsabilitats en matèria de seguretat en l'etapa de reclutament de personal i incloure-les en els acords a signar-se i verificar el seu compliment durant l'acompliment de l'individu com a empleat, així com, garantir que els usuaris estiguin al corrent de les amenaces i incumbències en matèria de seguretat de la informació, i es trobin capacitats per a recolzar la política de seguretat de l'organització en el transcurs de les seves tasques normals.

- **Gestió d'actius**

L'objectiu del present domini és que l'organització tingui coneixement precís sobre els actius que posseeix com a part important de l'administració de riscos.

Els actius d'informació han de ser classificats d'acord amb la sensibilitat i criticitat de la informació que contenen o bé d'acord amb la funcionalitat que compleixen i retolats en funció a això, a fi d'assenyalar com ha de ser tractada i protegida aquesta informació.

Les pautes de classificació han de preveure i contemplar el fet que la classificació d'un ítem d'informació determinat no necessàriament ha de mantenir-se invariable per sempre, i que aquesta pot canviar d'acord amb una política predeterminada per la pròpia organització.

- **Control d'accés**

L'objectiu del present domini és controlar l'accés per mitjà d'un sistema de restriccions i excepcions a la informació com a base de tot sistema de seguretat informàtica.

Per a impedir l'accés no autoritzat als sistemes d'informació s'haurien d'implementar procediments formals per a controlar l'assignació de drets d'accés als sistemes d'informació, bases de dades i serveis d'informació, i aquests han d'estar clarament documentats, comunicats i controlats quant al seu compliment.

Els procediments comprenen totes les etapes del cicle de vida dels accessos dels usuaris de tots els nivells, des del registre inicial de nous usuaris fins a la privació final de drets dels usuaris que ja no requereixen l'accés.

La cooperació dels usuaris és essencial per a l'eficàcia de la seguretat, per tant, és necessari conscienciar als mateixos sobre les seves responsabilitats pel manteniment de controls d'accés eficaços, en particular aquells relacionats amb l'ús de contrasenyes i la seguretat de l'equipament.

- **Xifratge**

L'objectiu del present domini és l'ús de sistemes i tècniques criptogràfiques per a la protecció de la informació sobre la base de l'anàlisi de risc efectuat, amb la

finalitat d'assegurar una adequada protecció de la seva confidencialitat i integritat.

L'aplicació de mesures de xifratge s'hauria de desenvolupar sobre la base d'una política sobre l'ús de controls criptogràfics i a l'establiment d'una gestió de les claus que sustenta l'aplicació de les tècniques criptogràfiques.

- **Seguretat física i ambiental**.

L'objectiu és minimitzar els riscos de danys i interferències a la informació i a les operacions de l'organització.

L'establiment de perímetres de seguretat i àrees protegides facilita la implementació de controls de protecció de les instal·lacions de processament d'informació crítica o sensible de l'organització, contra accessos físics no autoritzats.

El control dels factors ambientals d'origen intern i/o extern permet garantir el correcte funcionament dels equips de processament i minimitzar les interrupcions de servei.

La informació emmagatzemada en els sistemes de processament i la documentació continguda en diferents mitjans d'emmagatzematge, són susceptibles de ser recuperades mentre no estan sent utilitzats. És per això que el transport i la disposició final presenten riscos que han de ser avaluats, especialment en casos en els quals l'equipament pertanyent a l'organització estigui físicament fora del mateix (housing) o en equipament aliè que albergui sistemes i/o presti serveis de processament d'informació (hosting/cloud).

- **Seguretat en l'operativa.**

L'objectiu és controlar l'existència dels procediments d'operacions i el desenvolupament i manteniment de documentació actualitzada relacionada.

Addicionalment, s'hauria d'avaluar el possible impacte operatiu dels canvis previstos a sistemes i equipament i verificar la seva correcta implementació, assignant les responsabilitats corresponents i administrant els mitjans tècnics necessaris per a permetre la segregació dels ambients i responsabilitats en el processament.

Amb la finalitat d'evitar potencials amenaces a la seguretat del sistema o als serveis de l'usuari, seria necessari monitorar les necessitats de capacitat dels sistemes en operació i projectar les futures demandes de capacitat.

El control de la realització de les còpies de resguard d'informació, així com la prova periòdica de la seva restauració permeten garantir la restauració de les operacions en els temps de recuperació establerts i delimitar el període màxim de pèrdua d'informació assumible per a cada organització.

S'haurien de definir i documentar controls per a la detecció i prevenció de l'accés no autoritzat, la protecció contra programari maliciós i per a garantir la seguretat de les dades i els serveis connectats a les xarxes de l'organització.

Finalment, s'haurien de verificar el compliment de les normes, procediments i controls establerts mitjançant auditories tècniques i registres d'activitat dels sistemes (logs) com a base per al monitoratge de l'estat del risc en els sistemes i descobriment de nous riscos.

- **Seguretat en les telecomunicacions.**

L'objectiu és assegurar la protecció de la informació que es comunica per xarxes telemàtiques i la protecció de la infraestructura de suport.

La gestió segura de les xarxes, la qual pot abastar els límits organitzacionals, requereix l'acurada consideració del flux de dades, implicacions legals, monitoratge i protecció.

La informació confidencial que passa a través de xarxes públiques sol requerir controls addicionals de protecció.

Els intercanvis d'informació per part de les organitzacions s'haurien de basar en una política formal d'intercanvi i en línia amb els acords d'intercanvi, i hauria de complir amb qualsevol legislació rellevant.

- **Adquisició, desenvolupament i manteniment dels sistemes de la informació.**

L'objectiu és assegurar la inclusió de controls de seguretat i validació de dades en l'adquisició i el desenvolupament dels sistemes d'informació.

Definir i documentar les normes i procediments que s'aplicaran durant el cicle de vida dels aplicatius i en la infraestructura de base en la qual es recolzen.

Definir els mètodes de protecció de la informació crítica o sensible.

Aplica a tots els sistemes informàtics, tant desenvolupaments propis o de tercers, i a tots els sistemes operatius i/o programari que integrin qualsevol dels ambients administrats per l'organització on resideixin els desenvolupaments esmentats.

- **Gestió de tercers**

L'objectiu és implementar i mantenir el nivell apropiat de seguretat de la informació i el lliurament dels serveis contractats en línia amb els acords de lliurament de serveis de tercers.

L'organització ha de revisar la implementació dels acords, monitorar el seu compliment amb els estàndards i manejar els canvis per a assegurar que els serveis siguin lliurats per a satisfer tots els requeriments acordats amb terceres persones.

- **Gestió d'incidents.**

L'objectiu és garantir que els esdeveniments de seguretat de la informació i les febleses associats als sistemes d'informació siguin comunicats de manera tal que s'apliquin les accions correctives en el temps oportú.

Les organitzacions compten amb innombrables actius d'informació, cadascun exposat a sofrir incidents de seguretat. És necessari comptar amb una capacitat de gestió d'aquests incidents que permeti començar per la seva detecció, dur a terme el seu tractament i col·laborar en la prevenció de futurs incidents similars.

- **Gestió de la continuïtat del negoci**

L'objectiu és preservar la seguretat de la informació durant les fases d'activació, de desenvolupament de processos, procediments i plans per a la continuïtat de negoci i de tornada a la normalitat.

S'hauria d'integrar dins dels processos crítics de negoci, aquells requisits de gestió de la seguretat de la informació amb atenció especial a la legislació, les operacions, el personal, els materials, el transport, els serveis i les instal·lacions addicionals, alternatius i/o que estiguin disposats d'una manera diferent de l'operativa habitual.

S'haurien d'analitzar les conseqüències dels desastres, falles de seguretat, pèrdues de servei i la disponibilitat del servei i desenvolupar i implantar plans de contingència per a assegurar que els processos del negoci es poden restaurar en els terminis requerits les operacions essencials, mantenint les consideracions en seguretat de la informació utilitzada en els plans de continuïtat i funció dels resultats de l'anàlisi de riscos.

Haurien de dur-se a terme les proves pertinents (com ara proves sobre el paper, simulacres, proves de failover, etc.) per a: (a) mantenir els plans actualitzats, (b) augmentar la confiança de l'adreça en els plans i (c) familiaritzar als empleats rellevants amb les seves funcions i responsabilitats sota condicions de desastre.

Minimitzar els efectes de les possibles interrupcions de les activitats normals de l'organització associades a desastres naturals, accidents, falles en l'equipament, accions deliberades o altres fets, protegint els processos crítics mitjançant una combinació de controls preventius i accions de recuperació.

Instruir al personal involucrat en els procediments de represa i recuperació amb relació als objectius del pla, els mecanismes de coordinació i comunicació entre equips (personal involucrat), els procediments de divulgació en ús, els requisits de la seguretat, els processos específics per al personal involucrat i responsabilitats individuals.

- **Compliment**

El disseny, operació, ús i administració dels sistemes d'informació estan regulats per disposicions legals i contractuals.

Els requisits normatius i contractuals pertinents a cada sistema d'informació haurien d'estar degudament definits i documentats.

L'objectiu és complir amb les disposicions normatives i contractuals a fi d'evitar sancions administratives a l'organització i/o als empleats que incorrin en responsabilitat civil o penal com a resultat d'incompliments.

S'ha de revisar la seguretat dels sistemes d'informació periòdicament a l'efecte de garantir l'adequada aplicació de la política, normes i procediments de seguretat, sobre les plataformes tecnològiques i els sistemes d'informació.

10.2. Annex 2 – Procediment d'auditories internes.

Dins de la família de la normativa ISO 27000 hi trobam la ISO/IEC 27001, la qual detalla i proporciona els requisits per l'establiment, la implantació, el manteniment i la millora contínua d'un SGSI. Els sistemes de gestió estan basats en la implementació d'un procés continu de millora, que és conegut com a cicle PDCA o cicle de Deming. El cicle PDCA està format per quatre processos que es van repetint de manera iterativa per al control d'un sistema: planificar, implementar, comprovar i actuar. En aquest cicle calen auditories internes, o també anomenades de primera part, en la fase de comprovació. Com que el cicle PDCA s'ha de fer contínuament per a garantir el control correcte del procés en qüestió, la realització d'auditories també és contínua. Aquestes auditories no es realitzen de manera independent les unes de les altres, sinó que són organitzades pels responsables de gestionar la funció d'auditoria de l'empresa.

L'auditor o l'equip auditor és la persona o el grup de persones que han estat designades per a dur a terme periòdicament l'auditoria interna de l'empresa. L'auditor intern és un professional que es dedica a garantir el correcte funcionament de l'empresa, protegir i incrementar el seu valor, millorar la gestió de riscs, els controls interns i la governança a través de les seves recomanacions.

Les principals funcionalitats de l'auditor intern són les següents:

- Revisar que la informació significativa sobre els aspectes financers, administratius i operatius sigui exacte, confiable i adequada.
- Analitzar l'acompliment de la plantilla laboral i verifica si compleix amb les polítiques, regulacions i procediments establerts.
- Verificar que els recursos adquirits són utilitzats i protegits amb eficàcia.
- Supervisar que els programes, plans i objectius de l'empresa s'aconsegueixin.
- Controlar la qualitat i els processos de millora.
- Corroborar que es reconeixen i dirigeixin adequadament els assumptes significatius en matèria legal i reguladora.
- Mesurar si s'estan complint els procediments obligatoris.
- Calcular els riscs estratègics de l'empresa i verificar si són gestionats adequadament.
- Avaluar totes les evidències i proporcionar una conclusió independent sobre els sistemes, processos, polítiques i reglaments.

Totes aquestes accions permetran a l'auditor conèixer les debilitats de l'empresa i poder emetre suggeriments a la junta directiva per superar-les.

L'equip auditor estarà format per tres membres amb els respectius rols:

- Auditor cap: és designat per la direcció del programa d'auditoria i és el responsable total del resultat de l'auditoria. L'auditor cap cal que tengui coneixements en tots els sistemes i que tengui habilitats addicionals de la resta de l'equip.
- Auditors: estan sota la direcció de l'auditor cap. Els auditors han de tenir coneixements específics sobre l'àmbit de l'activitat auditada, capacitat

per entendre les situacions i coneixement sobre la legislació aplicable i els reglaments.

- Experts: estan sota la direcció de l'auditor cap. Els experts tècnics presenten habilitats tècniques específiques que són necessàries per executar certes proves d'auditoria que no els cobreix l'equip auditor.

Per tal d'aconseguir la certificació ISO/IEC 27001:2013, l'empresa haurà de realitzar una sèrie d'auditories internes, les quals s'hauran de revisar en el temps segons l'evolució de la norma.

Com a mínim l'empresa realitzarà una auditoria a l'any completa, i durant l'any realitzarà auditories parcials on s'aniran revisant els diferents controls que estan detallats a la normativa ISO/IEC 27002:2013. A continuació a la següent taula hi trobam la planificació d'auditoria a realitzar durant un any.

Planificació d'auditories												
Control	Mes de realització											
	1	2	3	4	5	6	7	8	9	10	11	12
5. Polítiques de seguretat de la informació	■											
6. Organització de la seguretat de la informació		■										
7. Seguretat relativa als recursos humans		■										
8. Gestió d'actius			■									
9. Control d'accés				■								
10. Criptografia					■							
11. Seguretat física de l'entorn						■						
12. Seguretat de les operacions							■					
13. Seguretat de les comunicacions							■					
14. Adquisició, desenvolupament i manteniment dels sistemes de la informació								■				
15. Relació amb els proveïdors									■			
16. Gestió dels incidents de seguretat de la informació										■		
17. Aspectes de seguretat de la informació per la gestió de la continuïtat de negoci											■	
18. Compliment												■

Per poder registrar les activitats previstes a l'auditoria interna i portar un control d'aquestes, és essencial que l'auditor elabori un informe d'auditoria. L'empresa té un model d'informe el qual serà utilitzat per a totes les auditories internes que es duguin a terme a l'empresa.

Informe auditoria interna (Nom de l'empresa – logotip de l'empresa)	
Versió:	**Codi**:
Data:	**Localització**:
Equip auditor:	
Abast de l'auditoria:	
Objectius de l'auditoria:	
Activitats desenvolupades:	
Resultats auditoria (No conformitat / Observacions / Oportunitats de millora):	
Observacions:	
Conclusions:	
Nom de l'auditor / DNI / Firma	

10.3. Annex 3 – Gestió d'indicadors.

Els indicadors bàsicament consisteixen en un conjunt de valors que s'obtenen mitjançant la comparació de punts de referència. Aquests indicadors de gestió es podran utilitzar a l'interior de l'entitat per mesurar l'efectivitat, l'eficàcia i l'eficiència dels components d'implementació i de gestió definits en el model d'operació del marc de la seguretat de la informació dins de l'empresa.
Haver de crear un indicador per a cada control de la norma ISO seria una tasca laboriosa i poc pràctica, per això es defineixen una sèrie d'identificadors que serviran per avaluar múltiples controls.

Els indicadors que s'utilitzen són els descrits pel MINTIC (Ministeri de Tecnologies de la Informació i Comunicacions) [2], el qual ha desenvolupat una guia d'indicadors, els quals es poden utilitzar en un SGSI d'una entitat pública tan privada.

A continuació es defineixen els indicadors:

<table>
<tr><th colspan="3">Indicador 01 – Organització de la seguretat de la informació</th></tr>
<tr><td>Identificador</td><td colspan="2">IN01</td></tr>
<tr><td colspan="3">Definició:
L'indicador ofereix la possibilitat d'identificar i fer un seguiment al compromís de la direcció de l'empresa enfront de la seguretat de la informació. A més, permet designar quins seran els responsables d'aquest tema dins de l'empresa.</td></tr>
<tr><td colspan="3">Objectiu:
Realitzar un seguiment a l'assignació de recursos i disponibilitats en gestió de la seguretat de la informació.</td></tr>
<tr><td>Tipus d'indicador:</td><td colspan="2">Identificador de gestió</td></tr>
<tr><td>Descripció variables</td><td>Fórmula</td><td>Font de la informació</td></tr>
<tr><td>VAR011: Nombre de treballadors de l'àrea de seguretat actuals.

VAR012: Nombre de treballadors de l'àrea de seguretat al cap d'un any.</td><td>(VAR011/VAR012)*100</td><td>Departament de recursos humans.</td></tr>
<tr><td>Meta mínima: 70-75%</td><td>Meta satisfactòria: 85%</td><td>Meta excel·lent: 100%</td></tr>
<tr><td colspan="3">Observacions:
L'indicador està enfocat a la contractació de noves persones i a l'assignació de responsabilitats.</td></tr>
</table>

Indicador 02 – Cobriment del SGSI en actius de la informació		
Identificador	IN02	
Definició: L'identificador ofereix la possibilitat de dur a terme el seguiment dels actius crítics de la informació i els controls que tenen relacionats a ells.		
Objectiu: Realitzar un seguiment dels actius crítics, existents i dels nous, de la informació i el seu control, dins del marc de la seguretat i la privacitat de la informació.		
Tipus d'indicador:	Identificador de gestió	
Descripció variables	**Fórmula**	**Font de la informació**
VAR021: Nombre d'actius crítics de la zona de risc inacceptable i la implementació del control no requereix adquisició d'elements de hardware o software. VAR022: Nombre total d'actius crítics identificats.	(VAR021/VAR022)*100	Inventari d'actius de la informació, pla de tractament i matriu de riscs. Inventari d'actius d'informació i actius recents.
Meta mínima: 75-80%	**Meta satisfactòria:** 85%	**Meta excel·lent:** 100%
Observacions: L'indicador ha de representar l'estat a nivell d'empresa. Està enfocat en realitzar una correcta classificació dels actius, tractaments, l'avaluació del risc associat i determinar els controls per tal de minimitzar el risc calculat.		

Indicador 03 – Tractament d'esdeveniments relacionats en el marc de seguretat i privacitat de la informació		
Identificador	IN03	
Definició: L'identificador pot determinar com es troba el tractament d'esdeveniments relacionats a la seguretat de la informació. Els esdeveniments seran facilitats pels usuaris o les auditories que es duguin a terme en el sistema.		
Objectiu: Reflectir la gestió i l'evolució del model de seguretat i privacitat de la informació dins de l'empresa.		
Tipus d'indicador:	Identificador de gestió	
Descripció variables	**Fórmula**	**Font de la informació**
VAR031: Nombre d'anomalies tancades.	(VAR031/VAR032)*100	Personal de seguretat i auditories internes

VAR032: Nombre total d'anomalies trobades.		
Meta mínima: 75%	**Meta satisfactòria:** 85%	**Meta excel·lent:** 100%
Observacions: -		

Indicador 04 – Pla de sensibilització		
Identificador	IN05	
Definició: L'indicador permet mesurar la sensibilitat en termes de seguretat de la informació per part dels usuaris. Aquesta mesura es podrà fer mitjançant les auditories.		
Objectiu: Establir l'efectivitat d'un pla de capacitació i sensibilització prèviament definit com un medi de control d'incidents de la seguretat.		
Tipus d'indicador:	Indicador de gestió	
Descripció variables	**Fórmula**	**Font de la informació**
VAR051: Nombre de falles trobades en les sensibilitzacions programades. VAR052: Nombre total del personal a capacitar.	(VAR051/VAR052)*100	Personal de seguretat i auditories internes. Inventari total dels treballadors de l'empresa.
Meta mínima: 80%	**Meta satisfactòria:** 90%	**Meta excel·lent:** 100%
Observacions: Per obtenir la informació pel mesurament, el responsable ha de crear activitats que permetin mesurar la capacitat de sensibilització.		

Indicador 05 – Compliment de polítiques dins de l'empresa		
Identificador	IN05	
Definició: L'identificador permet complir de manera eficaç les polítiques de seguretat de la informació de l'empresa plantejades.		
Objectiu: Trobar el nivell d'estructuració dels processos de l'empresa orientats a la seguretat de la informació.		
Tipus d'indicador:	Indicador de compliment	
Descripció de variables	**Fórmula**	**Font de la informació**
VAR051: L'empresa té		Política de seguretat de

definida una política de seguretat de la informació? VAR052: L'empresa compleix els requisits legals, reglamentaris i contractuals sobre el maneig de la informació?	Sí = 1 No = 0	l'empresa i els usuaris interns.
Meta:	Compleix: 1	No compleix: 0
Observacions:	**-**	

Indicador 06 – Identificació d'alineament de seguretat de l'entitat		
Identificador	IN06	
Definició: L'identificador pretén calcular el grau de la seguretat de la informació i dels equips de còmput utilitzats.		
Objectiu: Avaluar la capacitat del recurs humà sobre un tema i els equips que s'utilitzaran per a aquest procés.		
Tipus d'indicador:	Indicador de compliment	
Descripció variables	**Fórmula**	**Font de la informació**
VAR061: L'empresa té definits alineaments de treball mitjançant el responsable de seguretat? VAR062: L'empres té definits alineaments sobre la protecció de les instal·lacions, els equips i l'entorn?	Sí = 1 No = 0	Personal de seguretat i usuaris interns.
Meta:	Compleix: 1	No compleix: 0
Observacions:	-	

Indicador 07 – Verificació del control d'accés	
Identificador	IN07
Definició: L'identificador pretén mesurar el grau de control d'accés de l'empresa.	
Objectiu: Identificar si existeixen normes o polítiques relacionades amb el control d'accés de l'empresa.	

Tipus d'indicador:	Identificador de compliment	
Descripció de variables	**Fórmula**	**Font de la informació**
VAR071: L'empresa té definides normes o estàndards per controlar l'accés dels usuaris? VAR072: L'empresa té una política sobre l'ús i accés a la informació de l'empresa? VAR073: L'empresa té controlat els dispositius mòbils i l'accés remot als recursos de l'empresa?	Sí = 1 No = 0	Política de seguretat i els usuaris interns.
Meta:	Compleix: 1	No compleix: 0
Observacions:	**-**	

Indicador 08 – Adquisició i manteniment del software		
Identificador	IN08	
Definició: L'identificador permet mesurar el grau de protecció dels serveis de l'empresa.		
Objectiu: Verificar el grau de protecció de la infraestructura tecnològica de l'empresa mitjançant la comprovació de l'existència de normes o estàndards d'adquisició o desenvolupament de les aplicacions.		
Tipus d'indicador:	Identificador de compliment	
Descripció variables	**Fórmula**	**Font de la informació**
VAR081: L'empresa té definides normes o estàndards per la gestió d'incidents relacionats amb el servei?	Sí = 1 No = 0	Política de seguretat i usuaris interns.
Meta:	Compleix: 1	No compleix: 0
Observacions:	**-**	

Indicador 09 – Implementació dels processos de registre i auditoria	
Identificador	IN09
Definició: L'indicador permet mesurar el grau d'existència de normes relacionades amb el registre i l'auditoria de seguretat de la informació.	

Objectiu: Identificar l'existència de normes o estàndards relacionats amb el registre i l'auditoria de la seguretat de la informació.		
Tipus d'indicador:	Indicador de compliment	
Descripció de variables	**Fórmula**	**Font de la informació**
VAR091: L'empresa té normes o estàndards pel registre i control d'esdeveniments del sistema? VAR092: L'empresa verifica de manera interna periòdicament els processos relacionats amb la seguretat i els sitemes?	Sí = 1 No = 0	Política de seguretat i usuaris interns.
Meta:	Compleix: 1	No compleix: 0
Observacions:	-	

Indicador 10 – Polítiques de privacitat i de confidencialitat		
Identificador	IN10	
Definició: L'identificador permet mesurar el grau d'implementació de les polítiques implementades dins de l'empresa en relació amb la privacitat i confidencialitat de la informació de l'empresa.		
Objectiu: Identificar el nivell d'implementació de les polítiques de privacitat i de confidencialitat de l'empresa.		
Tipus d'indicador:	Indicador de compliment	
Descripció variables	**Fórmula**	**Font de la informació**
VAR101: L'empresa té implementades normes o estàndards per protegir la informació dels usuaris dels seus serveis? VAR102: L'empresa té implementades normes o estàndards per protegir la informació de les entitats que utilitzen els seus serveis?	Sí = 1 No = 0	Política de seguretat i usuaris interns.

Meta:	Compleix: 1	No compleix: 0
Observacions:	**-**	

Indicador 11 – Polítiques d'integritat de la informació		
Identificador	IN11	
Definició: L'indicador pretén mesurar el grau d'implementació dels mecanismes per la integritat de la informació de l'empresa.		
Objectiu: Identificar el nivell d'implementació de les polítiques de privacitat i confidencialitat per tal de mantenir la integritat de la informació de l'empresa.		
Tipus d'indicador:	Identificador de compliment	
Descripció variables	**Fórmula**	**Font de la informació**
VAR111: L'empresa té implementats alineaments contra la modificació o pèrdua d'informació? VAR112: L'empresa té implementades normes o estàndards per recuperar la informació en cas de modificació o pèrdua?	Sí = 1 No = 0	Política de seguretat i usuaris interns.
Meta:	Compleix: 1	No compleix: 0
Observacions:	**-**	

Indicador 12 – Disponibilitat del servei		
Identificador	IN12	
Definició: L'indicador pretén mesurar el grau de compliment de les polítiques de disponibilitat del servei.		
Objectiu: Identificar i verificar el grau d'implementació de les polítiques de disponibilitat del servei, és a dir, el grau de disponibilitat del servei.		
Tipus d'indicador:	Identificador de compliment	
Descripció variables	**Fórmula**	**Font de la informació**
VAR121: L'empresa verifica que les normes o estàndards orientats a la continuïtat en la	Sí = 1 No = 0	Política de seguretat i usuaris interns

prestació de serveis es compleixen? VAR122: L'empresa implementa mecanismes perquè els serveis tenguin alts índexs de disponibilitat?		
Meta:	Compleix: 1	No compleix: 0
Observacions:	-	

Indicador 13 – Atacs informàtics a l'empresa		
Identificador	IN13	
Definició: L'identificador pretén calcular el percentatge d'atacs informàtics rebuts a l'empresa, els quals varen impedir la prestació d'algun dels seus serveis.		
Objectiu: Revelar la probabilitat de què l'empresa pugui sofrir algun tipus d'amenaça.		
Tipus d'indicador:	Identificador de compliment	
Descripció variables	**Fórmula**	**Font de la informació**
VAR131: Quants d'atacs informàtics ha sofert l'empresa en el darrer any? VAR132: Quants d'atacs ha sofert l'empresa en el darrer any que han impedit l'ús d'algun dels serveis que ofereix l'empresa?	Sí= 1 No= 0	Eines de monitorieg i usuaris interns.
Meta:	Compleix: 1	No compleix: 0
Observacions:	-	

Indicador 14 – Implementació dels controls	
Identificador	IN14
Definició: L'indicador permet mesurar el grau d'avanç en la implementació dels controls de seguretat.	
Objectiu: Avaluar la implementació dels controls dins del sistema de gestió de la seguretat de la informació.	

Tipus d'indicador:	Indicador de gestió	
Descripció variables	**Fórmula**	**Font de la informació**
VAR141: Nombre de controls implementats. VAR142: Nombre de controls que es varen plantejar per implementar.	(VAR141/VAR142)*100	Pla de tractament de riscs
Meta mínima: 75%	**Meta satisfactòria**: 85%	**Meta excel·lent**:100%
Observacions:	**-**	

La informació que s'obtindrà després d'haver aplicat aquests indicadors haurà de ser interpretada pel departament de seguretat sota la supervisió del responsable de seguretat de l'empresa. A partir dels resultats obtinguts, sorgiran propostes de millora, eliminació o implementació de nous controls, els quals permetran realitzar un seguiment més acurat del SGSI.

10.4. Annex 4 – Procediment de revisió per direcció.

És fonamental fer revisions periòdiques del Sistema de Gestió de la Seguretat de la Informació per part de la direcció de l'empresa amb l'objectiu de comprovar el bon funcionament del sistema i si s'estan complint els objectius segons la normativa ISO/IEC 27001.

Tal com diu l'apartat 9.3 de la norma ISO/IEC 27001:2013 titulat "Revisió per la direcció":

La direcció de l'empresa ha de revisar el SGSI de l'organització a intervals planificats, per tal d'assegurar-se que la convivència, l'adequació i l'eficàcia són contínues.

La revisió per part de la direcció ha d'incloure consideracions sobre:

- L'estat de les accions en relació amb les revisions prèvies per l'organització.
- Els canvis en les qüestions internes i externes que siguin pertinents al SGSI.
- La informació sobre el comportament de la seguretat de la informació, incloses les tendències relatives a: (1) no conformitats i accions correctives, (2) seguiment i resultats de les mesures, (3) resultats d'auditoria i (4) el compliment dels objectius de la seguretat de la informació.
- Els comentaris provinents de les parts interessades.
- Els resultats de la valoració de riscs i l'estat del pla de tractament de riscos.
- Les oportunitats de millora continua.

Com a punts de sortida de la revisió per direcció s'han de considerar les decisions relacionades amb les oportunitats de millora i les necessitats de canvi estratègiques.

A més, l'organització ha de guardar la informació documentada com evidència dels resultats de les revisions realitzades per la direcció.

Els punts d'entrada que s'han de tenir en compte per a la realització de la revisió per la direcció són els següents:

- Resultat de les auditories internes.
- Resultats de les enquestes de satisfacció del client.
- Funcionament del sistema de gestió de qualitat.
- Planificació del sistema de gestió de qualitat.
- Estat de les accions correctives i preventives.
- Seguiment de les accions derivades de revisions anteriors.
- Canvis que puguin afectar el sistema de gestió de qualitat.
- Recomanacions per la millora del SGSI.
- Revisió de la política de qualitat i els objectius de qualitat.

Les revisions per direcció estan planificades per realitzar-se anualment, o de manera extraordinària quan la direcció de l'empresa ho consideri, les quals segueixen la següent planificació.

Planificació de revisions per direcció												
Control	Mes de realització											
	1	2	3	4	5	6	7	8	9	10	11	12
5. Polítiques de seguretat de la informació	■											
6. Organització de la seguretat de la informació	■											
7. Seguretat relativa als recursos humans	■											
8. Gestió d'actius				■								
9. Control d'accés				■								
10. Criptografia				■								
11. Seguretat física de l'entorn							■					
12. Seguretat de les operacions							■					
13. Seguretat de les comunicacions							■					
14. Adquisició, desenvolupament i manteniment dels sistemes de la informació										■		
15. Relació amb els proveïdors										■		
16. Gestió dels incidents de seguretat de la informació												■
17. Aspectes de seguretat de la informació per la gestió de la continuïtat de negoci												■
18. Compliment						■						

El responsable de seguretat realitzarà un informe sobre la revisió del SGSI realitzada. En aquest informe apareixeran les incidències, les deficiències detectades i una relació de solucions i propostes de millora. Llavors el responsable de seguretat ha de convocar una reunió amb la direcció dins del termini establert, per tal d'informar sobre les revisions i perquè els informes puguin ser revisats. En cas de trobar-se davant un incident greu de seguretat, es convocarà una reunió urgent amb direcció on s'informarà dels fets per tal que el comitè de direcció prengui les decisions necessàries per garantir el bon funcionament i manteniment del sistema. De la mateixa manera que s'espera del comitè de direcció prengui les decisions per tal de millorar l'eficiència del SGSI.

L'empresa té un model d'informe el qual servirà de guia per deixar constància de les revisions per la direcció que es duguin a terme a l'empresa.

Informe de revisió per la direcció (Nom de l'empresa – logotip de l'empresa)	
Versió:	**Codi**:
Data:	**Localització**:
Equip de revisió:	
Abast de la revisió:	
Objectius de la revisió:	
Activitats desenvolupades:	
Resultats de la revisió / Conclusions:	
Noms dels revisors / DNI / Firma	

10.5. Annex 5 – Gestió de rols i responsabilitats.

Tal com diu la normativa ISO/IEC 27001:2013 a l'apartat 5.3, titulat "Rols, responsabilitats i autoritats a l'organització":

L'alta direcció ha d'assegurar-se que les responsabilitats i les autoritats pels rols pertinents a la seguretat de la informació s'assignen i es comuniquen dins de l'organització.

L'alta direcció ha d'assignar la responsabilitat i l'autoritat per:

a) Assegurar-se que el sistema de gestió de la seguretat de la informació es conforme amb els requisits d'aquesta norma internacional, i
b) Informar a l'alta direcció sobre el comportament del sistema de gestió de la seguretat de la informació.

Com hem comentat abans, el Comitè de Seguretat de la Informació està format pels següents rols: CEO, responsable de seguretat, responsable de ciberseguretat, responsable de recursos humans, responsable de comunicació i màrqueting, responsable d'IT, responsable financer, responsable fiscal i legal.

A continuació anem a analitzar els diferents rols i les responsabilitats de cadascun d'ells.

- CEO.
  El CEO és l'encarregat de coordinar totes les activitats de l'empresa, és a dir, supervisen l'acompliment dels empleats, controlen els pressuposts, estableixen els objectius generals, etc., a més d'assegurar-se que totes les activitats es realitzen de manera eficient, organitzada, segura i rendible.

- Responsable de seguretat.
  El responsable de seguretat és l'encarregat d'elaborar, promoure i mantenir la política de seguretat de la informació, d'elaborar un pla de riscs i les possibles solucions per mitigar les amenaces, promoure nous objectius relacionats en la seguretat de la informació, desenvolupar i mantenir el marc normatiu de seguretat i vetlar pel seu compliment, gestionar i analitzar les incidències de seguretat que ocorren a l'empresa, controlar que les auditories es realitzen en la freqüència adequada, i en general gestionar la seguretat de la informació de l'empresa de manera global.

- Responsable de recursos humans.
  El responsable de recursos humans és l'encarregat de reclutar nous treballadors per l'empresa, planificar el personal necessari per als diferents departaments de l'organització, dissenyar i implementar programes de formació i conscienciació sobre la seguretat de la informació, revisar els contractes de treball, nòmines, seguretat social, entre d'altres, dels treballadors, executar processos administratius o disciplinaris, implementar mesures de protecció i de prevenció i facilitar les relacions laborals entre sindicats.

- Responsable de comunicació i màrqueting.
  El responsable de comunicació i màrqueting és l'encarregat de gestionar la comunicació interna i externa de l'organització. Ha de definir la política de comunicació de l'empresa i el desenvolupament d'una estratègia, dissenyar accions de màrqueting per promoure l'empresa i els valors d'aquesta, desenvolupar contactes estrets amb els mitjans de comunicació i la premsa, negociar la publicitat, física i en línia, de l'empresa, administrar el pressupost assignat a les relacions públiques i comunicacions.

- Responsable d'IT.
  El responsable d'IT és l'encarregat d'avaluar les necessitats tecnològiques de l'organització i fer recomanacions d'actualitzacions, establir objectius d'implementació de les tecnologies de la informació a curt, mitjà i llarg termini, planificar i dirigir les modificacions a la infraestructura segons les necessitats de l'empresa, protegir els sistemes i les dades de les amenaces, gestionar el pressupost assignat al sistema d'IT, gestionar el personal d'IT (tècnics, desenvolupadors, especialistes, etc.).

- Responsable ciberseguretat.
  El responsable de ciberseguretat és l'encarregat de protegir tots els dispositius, servidors, aplicacions i dades de la companyia. D'alguna manera garanteix que la informació privada de l'empresa continua essent privada inclús quan ha viatjat a través d'Internet. Aquesta figura està dins del departament d'IT, perquè actualment no està prou desenvolupat per tenir entitat pròpia a l'empresa.

- Responsable financer.
  El responsable financer o CFO (Chief Financial Officer) és l'encarregat de la planificació i execució econòmica i financera de l'empresa, de gestionar la comptabilitat, de controlar la informació i les relacions financeres, de vetlar pel correcte ús dels recursos financers, d'establir estratègies a curt, mitjà i llarg termini.

- Responsable fiscal i legal.
  El responsable fiscal i legal és l'encarregat de proporcionar informació, assistència i representació a l'empresa, de vetlar pel correcte compliment de les liquidacions tributàries, de donar d'alta, de baixa o realitzar modificacions relatives a l'activitat econòmica de l'empresa, de revisar periòdicament la legislació vigent.

10.6. Annex 6 – Metodologia d'anàlisis de riscos.

Segons MAGERIT [5], l'anàlisi de riscos és una aproximació metòdica per determinar el risc seguint les següents passes:

1- Determinar els actius rellevants per l'organització, la interrelació i el seu valor, en el sentit de quin cost suposaria la seva degradació.
2- Determinar a quines amenaces estan exposats aquests actius.
3- Determinar quines salvaguardes hi ha disponibles i l'eficàcia que tenen enfront del risc.
4- Estimar l'impacte, definit com el dany sobre l'actiu derivat de la materialització de l'amenaça.
5- Estimar el risc, definit com l'impacte ponderat amb la taxa d'ocurrència de l'amenaça.

L'anàlisi de riscos es duu a terme mitjançant una anàlisi metòdica seguint els següents passos:

1- Actius: component d'un sistema d'informació que és susceptible a ser atacat deliberadament o accidentalment amb conseqüències per l'organització. Alguns dels actius són: la informació, les dades, les aplicacions, els equips, les comunicacions, els recursos administratius, els recursos físics i humans.

   Malgrat que s'hagi d'adaptar a cada organització que s'analitza, els actius es poden classificar en les següents capes, on les capes superiors depenen de les capes inferiors:
   - Actius essencials: la informació que es maneja i els serveis prestats.
   - Serveis interns que estructuren ordenadament el sistema d'informació.
   - Equipament informàtic: software, hardware, comunicacions i suports d'informació (USB, CD, etc.).
   - Entorn: equipament i subministrament, mobiliari.
   - Serveis subcontractats a tercers.
   - Instal·lacions físiques.
   - Personal: usuaris, operadors i administratius, desenvolupadors.

   Les dimensions que interessen calibrar d'un actiu són la confidencialitat, la integritat i la disponibilitat. També és interessant valorar l'autenticitat i la traçabilitat.

2- Amenaces: causa potencial d'un incident que pot causar danys a un sistema d'informació o a una organització.

   Les amenaces poden identificar en amenaces d'origen natural, d'origen industrial, de defectes de les aplicacions, causades per persones de manera accidental o de manera deliberada.

Quan s'ha determinat que una amenaça pot perjudicar a un actiu, s'ha de valorar el valor de l'actiu en dos sentits: la degradació (quant de perjudicat resultaria el valor de l'actiu) i la probabilitat (quant de probable o improbable és que es materialitzi l'amenaça).

3- Salvaguardes: procediment o mecanisme tecnològic que redueix el risc. Hi ha amenaces que es poden impedir organitzant-se adequadament, mentre que altres requereixen elements tècnics i altres seguretat física.

   Per seleccionar les salvaguardes hem de tenir en compte els següents aspectes:
   1- Tipus d'actiu a protegir, cada tipus es protegeix de manera específica.
   2- Dimensió o dimensions de seguretat que requereixen protecció.
   3- Amenaces de les quals necessitam protegir-nos.
   4- Si existeixen salvaguardes alternatives.

   A l'hora de seleccionar les salvaguardes per excloure s'ha d'analitzar si no aplica (no és d'aplicació perquè tècnicament no és adequada al tipus d'actiu a protegir) i si no es justifica (la salvaguarda aplica, però és desproporcionada pel risc que hem de protegir).

4- Impacte residual: donat un conjunt de salvaguardes desplegades i una mesura de la maduresa del procés de gestió, el sistema queda en una situació de possible impacte, que s'anomena impacte residual.

5- Risc residual: donat un conjunt de salvaguardes desplegades i una mesura de la maduresa del procés de gestió, el sistema queda en una situació de possible risc, que s'anomena risc residual.

10.7. Annex 7 – Declaració d'aplicabilitat.

La normativa ISO/IEC 27001:2013 ens diu que l'organització ha de determinar els límits i l'aplicabilitat del sistema de gestió de la seguretat de la informació per tal d'establir el seu abast. A l'hora d'elaborar una declaració d'aplicabilitat cal que aquesta contengui els controls necessaris, la justificació de les inclusions, si els controls necessaris estan implementats o no i la justificació de les exclusions de qualsevol control de la informació. [6]

	Control	Aplica?
A5	**Polítiques de seguretat de la informació**	
A5.1	**Direcció de gestió per a la seguretat de la informació** Nivell maduresa actual: 70%	
1.	La direcció ha publicat i aprovat les polítiques sobre la seguretat de la informació acordar amb els requisits del negoci? Justificació: Sí, la direcció ha publicat i aprovat les polítiques de seguretat de la informació i les ha comunicat als seus treballadors.	Sí
2.	Hi ha un procés planificat i verificable de revisió de les polítiques de seguretat de la informació? Justificació: Sí, s'ha realitzat una programació de les revisions que es duran a terme durant l'any.	Sí
A6	**Organització de la Seguretat de la Informació**	
A6.1	**Tractament de riscos i oportunitats** Nivell maduresa actual: 76%	
1.	S'han assignat i definit les responsabilitats sobre la seguretat de la informació en les tasques o activitats de l'organització? Justificació: Sí, els equips de treball estan definits segons les activitats i les respectives responsabilitats assignades a cada treballador.	Sí
2.	S'han segregat les diverses àrees de responsabilitat sobre la seguretat de la informació per evitar usos o accessos indeguts? Justificació: Sí, les tasques estan assignades per equips segons les responsabilitats que tenen assignades.	Sí
3.	Hi ha un procés definit per contactar amb les autoritats competents davant d'incidents relacionats amb la Seguretat de la Informació? Justificació: Sí, als contractes dels treballadors hi ha una clàusula específica relacionada amb la seguretat de la informació, la qual pretén mantenir la confidencialitat de les dades.	Sí
4.	Hi ha mitjans i s'han establert contactes amb grups d'interès i	

	associacions relacionades amb la seguretat de la informació per mantenir-se actualitzat a notícies i informació sobre seguretat? Justificació: Sí, als contractes dels treballadors hi ha una clàusula específica relacionada amb la seguretat de la informació, la qual pretén mantenir la confidencialitat de les dades.	Sí
5.	Hi ha requisits per fer front a qüestions sobre la seguretat de la informació en la gestió de projectes de l'organització? Justificació: Sí, hi ha una plantilla amb els requisits essencials per mantenir la seguretat de la informació.	Sí
A6.2	**Dispositius Mòbils i Teletreball** Nivell maduresa actual: 80%	
1.	Es consideren requisits especials per a la seguretat de la informació en la utilització de dispositius mòbils? Justificació: Sí, els treballadors tenen la documentació amb les recomanacions referents a l'ús de dispositius mòbils.	Sí
2.	S'apliquen els criteris de seguretat per als accessos de teletreball? Justificació: Sí, els treballadors tenen la documentació amb les recomanacions referents al teletreball, per tal de no posar en perill la informació de l'empresa.	Sí
A7	**Seguretat en els recursos humans**	
A7.1	**Abans de contractar un empleat** Nivell maduresa actual: 75%	
1.	S'investiguen els antecedents dels candidats? Justificació: Sí, es comprova que el treballador que s'ha seleccionat pel nou lloc de treball no presenta antecedents penals relacionats amb l'activitat que està a punt de començar.	Sí
2.	S'hi inclouen clàusules relatives a la Seguretat de la Informació en els contractes de treball? Justificació: Sí, als contractes de treball s'inclouen clàusules relatives a la seguretat de la informació perquè els treballadors coneguin quines són les penalitzacions en cas de no complir amb els termes de seguretat.	Sí
A7.2	**Durant el contracte** Nivell maduresa actual: 80%	
1.	El compliment de les responsabilitats sobre la Seguretat de la Informació és exigida de manera activa a empleats i contractistes? Justificació: Sí, s'exigeix als treballadors i contractistes el compliment de les responsabilitats.	Sí

2.	Hi ha processos d'informació, formació i sensibilització sobre les responsabilitats sobre la seguretat de la informació? Justificació: Sí, contínuament hi ha processos d'informació i formació per tal de tenir els treballadors al dia de les noves tecnologies i polítiques de seguretat. Els treballadors estan obligats a realitzar certs cursos a l'any per estar al dia.	Sí
3.	Hi ha un pla disciplinari on es comunica als empleats i contractistes les conseqüències dels incompliments sobre les polítiques de la Seguretat de la Informació? Justificació: Sí, existeix un procés d'obertura d'expedient i de seguiment del treballador de processos disciplinaris.	Sí
A7.3	**Terminació del contracte** Nivell maduresa actual: 70%	
1.	Hi ha un procediment per garantir la seguretat de la informació en els canvis d'ocupació, el lloc de treball o en finalitzar un contracte? Justificació: Sí, la informació del treballador està protegida en cas de veure's modificat el seu contracte de treball.	Sí
2.	Es defineixen responsabilitats sobre la seguretat de la informació que s'estenguin més enllà de la finalització d'un contracte com ara qüestions relatives a la confidencialitat de la informació? Justificació: Sí, en cap moment es pot rompre el compromís de confidencialitat estant treballant dins l'empresa o un cop finalitzada l'activitat en ella.	Sí
A8	**Gestió d'actius**	
A8.1	**Responsabilitat sobre els Actius** Nivell maduresa actual: 85%	
1.	S'ha fet un inventari d'actius que donen suport al negoci i d'informació? Justificació: Sí, es duen a terme inventaris d'actius mitjançant l'eina de gestió *proactivanet*.	Sí
2.	S'ha identificat el responsable de cada actiu quant a seguretat? Justificació: Sí, a l'inventari d'actius apareix la propietat de cadascun d'ells.	Sí
3.	S'han establert normes per a l'ús d'actius en relació amb la seguretat? Justificació: Sí, els treballadors coneixen la política d'ús acceptable dels actius en relació amb la seguretat.	Sí
4.	Hi ha procediment per a la devolució d'actius cedits a terceres parts o a la finalització d'un lloc de treball o contracte?	Sí

	Justificació: Sí, a la política d'ús acceptable dels actius hi apareix la clàusula que indica que un cop finalitzada l'activitat amb l'empresa, tots els dispositius han de ser retornats en bon estat.	
A8.2	**Classificació de la informació** Nivell maduresa actual: 90%	
1.	Es classifica la informació segons la seva confidencialitat o la seva importància amb vista a establir mesures de seguretat especifiques? Justificació: Sí, només es classifica la informació a certs nivells de la companyia.	Sí
2.	Els actius d'informació són fàcilment identificables quant al grau de confidencialitat o al nivell de classificació? Justificació: Sí, només es classifica la informació a certs nivells de la companyia.	Sí
3.	Hi ha procediments per manipular la informació d'acord amb la classificació? Justificació: Sí, només per a certs nivells de la companyia.	Sí
A8.3	**Manipulació de suports** Nivell maduresa actual: 65%	
1.	Hi ha controls establerts per aplicar a suports extraïbles? -Ús -Xifrat -Esborrat -Etc. Justificació: Sí, hi ha polítiques establertes per l'ús, el control i l'auditoria dels dispositius extraïbles.	Sí
2.	Hi ha procediments establerts per a l'eliminació de suports? Justificació: Sí, hi ha procediments establerts per l'eliminació de suports.	Sí
3.	Hi ha procediments per al trasllat de suports d'informació per protegir-ne la seguretat? - Control de sortides -Xifrat etc. Justificació: Sí, hi ha procediments establerts que es troben en procés de millora.	Sí
A9	**Control d'accés**	
A9.1	**Requisits generals per al control d'accés** Nivell maduresa actual: 90%	
1.	Hi ha una política per definir els controls d'accés a la informació que tinguin en compte l'accés selectiu a la informació segons les necessitats de cada activitat o lloc de treball? Justificació: Sí, la direcció ha publicat i aprovat les polítiques	Sí

	relacionades amb el control d'accés i les ha comunicat als seus treballadors.	
2.	S'estableixen accessos limitats als recursos i les necessitats de xarxa segons perfils determinats? Justificació: Sí, s'han definit els límits dels accessos als recursos a la política i s'han implementat estratègies de segmentació de la xarxa.	Sí
A9.2	**Accessos d'usuari** Nivell maduresa actual: 80%	
1.	Hi ha processos formals de registre d'usuaris? Justificació: Sí, hi ha processos formals definits pel departament d'IT que controlen el registre d'usuaris.	Sí
2.	Hi ha processos formals per assignar perfils d'accés? Justificació: Sí, hi ha processos formals definits pel departament d'IT que controlen el registre d'usuaris i la seva assignació.	Sí
3.	Es defineix un procés específic per a l'assignació i l'autorització de permisos especials d'administració d'accessos? Justificació: Sí, hi ha processos formals definits pel departament d'IT que controlen l'assignació de perfils i els respectius privilegis.	Sí
4.	S'ha establert una política específica per al maneig d'informació classificada com a secreta? Quant a: autenticació i compromisos. Justificació: Sí, a la política de la seguretat de la informació es contemplen totes les modalitats d'informació.	Sí
5.	S'estableixen períodes concrets per a la renovació dels permisos d'accés? Justificació: Sí, l'empresa té una planificació anual definida per revisar i renovar els permisos d'accés.	Sí
6.	Hi ha un procés definit per a la revocació de permisos quan es finalitzi una activitat, lloc de treball o cessament de contractes? Justificació: Sí, a la política de la seguretat de la informació es contempla el fi de l'activitat dels treballadors.	Sí
A9.3	**Responsabilitats dels usuaris** Nivell maduresa actual: 90%	
1.	S'estableixen normes per a la creació i la salvaguarda de contrasenyes d'accés? Justificació: Sí, s'han implementat procediments per controlar l'accés.	Sí

A9.4	**Control d'accés a sistemes i aplicacions** Nivell maduresa actual: 90%	
1.	S'estableixen nivells i perfils específics d'accés per als sistemes d'informació de manera que la informació es restringeixi a l'activitat específica a desenvolupar? Justificació: Sí, s'han implementat procediments per controlar l'accés.	Sí
2.	S'han implementat processos d'accés segur per iniciar sessió considerant limitacions d'intents d'accés, controlant la informació en pantalla, etc.? Justificació: Sí, s'han implementat procediments per controlar l'accés.	Sí
3.	S'estableixen mesures per controlar l'establiment de contrasenyes segures? Justificació: Sí, totes les contrasenyes han de complir uns requisits mínims per tal que siguin segures.	Sí
4.	Es controla la capacitació i el perfil de les persones que tenen permisos d'administració amb perfils baixos de seguretat? Justificació: Sí, hi ha procediments establerts que es troben en procés de millora.	Sí
5.	L'accés a codis font de programes es restringeix i es controla qualsevol tipus de canvi a realitzar? Justificació: Sí, l'accés als codis fonts està restringit i és controlat pel sistema de gestió d'aquest.	Sí
A10	**Criptografia**	
A10.1	**Control criptogràfic** Nivell maduresa actual: 80%	
1.	Hi ha una política per a l'establiment o no de controls criptogràfics? Justificació: Sí, a la política de seguretat interna es contempla l'ús de controls criptogràfics.	Sí
2.	Hi ha un control del cicle de vida de les claus criptogràfiques? Justificació: Sí, està contemplat dins l'apartat d'ús de controls criptogràfics a la política de seguretat.	Sí
A11	**Seguretat física i de l'entorn**	
A11.1	**Àrees de seguretat** Nivell maduresa actual: 85%	
1.	S'estableixen perímetres de seguretat física on calgui amb barreres d'accés? Justificació: Sí, hi ha implementades mesures físiques de seguretat en el perímetre d'accés de l'empresa.	Sí
2.	Hi ha controls d'accés a persones autoritzades en àrees	Sí

	restringides? Justificació: Sí, hi ha mesures de control d'accés físic a les oficines centrals de l'empresa, com per exemple al CPD i als despatxos.	
3.	S'estableixen mesures de seguretat per a zones d'oficines per protegir la informació de pantalles, etc. a àrees d'accessibles a personal extern? Justificació: Sí, hi ha mesures de control d'accés físic a les oficines centrals de l'empresa.	Sí
4.	L'activitat de personal que accedeix a àrees segures es controla o supervisa? Justificació: Sí, hi ha mesures de control d'accés físic a les oficines centrals de l'empresa i es realitza una auditoria dels fitxers de control d'accés.	Sí
5.	Es controlen les àrees de Càrrega i descàrrega amb procediments de control de mercaderies lliurades, etc.? Justificació: A les oficines centrals no hi ha una zona de càrrega i descàrrega.	No
A11.2	**Seguretat dels equips** Nivell maduresa actual: 75%	
1.	Es protegeixen els equips tant del medi ambient com dels accessos no autoritzats? Justificació: Sí, hi ha mesures de control d'accés dels dispositius. Els dispositius no estan exposats a inclemències climàtiques.	Sí
2.	Els equips es protegeixen contra fallades de subministrament d'energia? Justificació: Sí, el sistema de subministrament està correctament instal·lat i posat a prova.	Sí
3.	Hi ha proteccions per als cablejats d'energia i de dades? Justificació: Sí, el cablejat de l'oficina està correctament instal·lat i compleix tots els certificats reglamentaris.	Sí
4.	Es planifiquen i fan tasques de manteniment sobre els equips? Justificació: Sí, hi ha una programació per revisar l'estat dels equips.	Sí
5.	Es controlen i s'autoritzen la sortida d'equips, aplicacions, etc. Que puguin contenir informació? Justificació: Sí, els equips poden ser trets pel responsable de l'actiu amb un motiu justificat.	Sí
6.	Es consideren mesures de protecció específiques per a	

	equips que s'utilitzin fora de les instal·lacions de la pròpia empresa? Justificació: Sí, es contempla a la política d'ús acceptable dels actius.	Sí
7.	S'estableixen protocols per protegir o eliminar informació d'equips que causen baixa o seran reutilitzats? Justificació: Sí, hi ha un protocol d'eliminació d'informació i l'empresa té contractada una empresa certificada per la destrucció dels equips.	Sí
8.	S'estableixen normes per protegir la informació dels equips quan els usuaris abandonen el lloc de treball? Justificació: Sí, es contempla a la política d'ús acceptable dels actius. Després d'un temps determinat d'inutilització es bloqueja la sessió del dispositiu.	Sí
9.	S'estableixen regles de comportament per a abandonaments momentanis o temporals del lloc de treball? Justificació: Sí, es contempla a la política d'ús acceptable dels actius. Després d'un temps determinat d'inutilització es bloqueja la sessió del dispositiu.	Sí
A12	**Seguretat a les operacions**	
A12.1	**Procediments i responsabilitats** Nivell maduresa actual: 85%	
1.	Es documenten els procediments i s'hi estableixen responsabilitats? Justificació: Sí, existeixen documents sobre les operacions a realitzar.	Sí
2.	Es controla que la informació sobre procediments es mantingui actualitzada? Justificació: Sí, hi ha definits procediments que indiquen com mantenir la informació actualitzada.	Sí
3.	Es disposa d'un procediment per avaluar l'impacte en la seguretat de la informació davant de canvis en els procediments? Justificació: Sí, estan documentats els processos implementats, però es troba en un procés de millora.	Sí
4.	Es controla l'ús dels recursos quant al rendiment i la capacitat dels sistemes? Justificació: Sí, hi ha un control monitoritzat de l'ús dels recursos.	Sí
5.	Els entorns de desenvolupament i proves estan convenientment separats dels entorns de producció?	Sí

	Justificació: Sí, l'entorn de desenvolupament i proves i l'entorn de producció són totalment independents.	
A12.2	**Protecció contra software maliciós** Nivell maduresa actual: 90%	
1.	Hi ha sistemes de detecció per a programari maliciós o codi maliciós? Justificació: Sí, els sistemes són analitzats per tal de detectar intrusions al sistema.	Sí
A12.3	**Còpies de seguretat** Nivell maduresa actual: 95%	
1.	S'ha establert un sistema de còpies de seguretat d'acord amb les necessitats de la informació i dels sistemes? Justificació: Sí, es realitzen còpies de seguretat diàries i immutables.	Sí
A12.4	**Registres i supervisió** Nivell maduresa actual: 90%	
1.	Es fa un registre d'esdeveniments? -Intents d'accés fallits/exitosos -Desconnexions del sistema -Alertes de fallades. Etc. Justificació: Sí, s'utilitza el sistema de registre del sistema operatiu i de les pròpies aplicacions.	Sí
2.	S'ha establert un sistema de protecció per als registres amb segregació de tasques o còpies de seguretat? Justificació: Sí, es realitzen còpies de seguretat diàries i immutables.	Sí
3.	Es protegeix convenientment i de manera específica els accessos o els dels administradors? Justificació: Sí, hi ha una política d'accessos per capes.	Sí
4.	Hi ha un control de sincronització dels diferents sistemes? Justificació: Sí, hi ha un control de sincronització que encara no està en funcionament per a tots els sistemes.	Sí
A12.5	**Control del software** Nivell maduresa actual: 90%	
1.	Les instal·lacions de noves aplicacions SW o modificacions són verificades en entorns de prova i hi ha protocols de seguretat per a la seva instal·lació? Justificació: Sí, tota aplicació és provada abans de ser posada en funcionament.	Sí
A12.6	**Vulnerabilitat tècnica** Nivell maduresa actual: 75%	
1.	S'estableixen mètodes de control per a vulnerabilitats tècniques "hacking ètic", etc.?	Sí

	Justificació: Sí, hi ha auditories de control per evitar sofrir vulnerabilitats en el sistema.	
2.	S'estableixen mesures restrictives per a la instal·lació de programari quant a personal autoritzat evitant les instal·lacions per part d'usuaris finals? Justificació: Sí, només poden fer instal·lacions de programari els treballadors que estan autoritzats, generalment del departament d'IT.	Sí
A12.7	**Auditories de sistemes d'informació** Nivell maduresa actual: 85%	
1.	Hi ha mecanismes d'auditories de mesures de seguretat dels sistemes? Justificació: Sí, hi ha mecanismes per mesurar la seguretat del sistema.	Sí
2.	S'estableixen protocols específics per al desenvolupament d'auditories Software considerant el seu impacte als sistemes? Justificació: Sí, hi ha definits alguns procediments a seguir pel desenvolupament d'auditories.	Sí
A13	**Seguretat de les comunicacions**	
A13.1	**Seguretat de xarxes** Nivell maduresa actual: 80%	
1.	A l'entorn de xarxa es gestiona la protecció dels sistemes mitjançant controls de xarxa i elements connectats? Justificació: Sí, hi ha un NAC (Network Access Control) implementat.	Sí
2.	S'estableixen condicions de seguretat als serveis de xarxa tant propis com subcontractats? Justificació: Sí, hi ha condicions de seguretat als serveis de la xarxa.	Sí
3.	Hi ha separació o segregació de xarxes tenint en compte condicions de seguretat i classificació d'actius? Justificació: Sí, hi ha segregació de xarxes en funció de les activitats de les aplicacions.	Sí
A13.2	**Intercanvi d'informació** Nivell maduresa actual: 85%	
1.	S'estableixen polítiques i procediments per protegir la informació als intercanvis? Justificació: Sí, hi ha una política definida per les eines d'intercanvi d'informació.	Sí
2.	Es delimiten i estableixen acords de responsabilitat en intercanvis d'informació amb altres entitats?	Sí

	Justificació: Sí, hi ha una política definida per les eines d'intercanvi d'informació.	
3.	S'estableixen normes o criteris de seguretat a missatgeria electrònica? Justificació: Sí, hi ha una política definida per les eines d'intercanvi d'informació.	Sí
4.	S'estableixen acords de confidencialitat abans de fer intercanvis d'informació amb altres entitats. Justificació: Sí, hi ha una política definida per les eines d'intercanvi d'informació i a més s'ha de signar un NDA (Non-disclosure agreement).	Sí
A14	**Adquisició, desenvolupament i manteniment de sistemes d'informació**	
A14.1	**Intercanvi d'informació** Nivell maduresa actual: 80%	
1.	Es defineixen i documenten els requisits de seguretat de la informació per als nous sistemes d'informació? Justificació: Sí, existeixen els requisits de seguretat de la informació definits pel departament d'IT.	Sí
2.	S'especifiquen els requisits de seguretat de la informació en el disseny de nous sistemes? Justificació: Sí, existeixen els requisits de seguretat de la informació definits pel departament d'IT.	Sí
3.	Es consideren requisits de seguretat específics per a accessos externs o de xarxes públiques als sistemes d'informació? Justificació: Sí, existeixen els requisits de seguretat de la informació definits pel departament d'IT.	Sí
4.	S'estableixen mesures de protecció per a transaccions en línia? Justificació: Sí, s'estableixen mesures de protecció mitjançant aplicacions de transaccions en línia.	Sí
A14.2	**Seguretat en els processos de suport** Nivell maduresa actual: 80%	
1.	S'estableixen procediments que garanteixin el desenvolupament segur del programari? Justificació: Sí, s'utilitzen Quality Gates específics per seguretat.	Sí
2.	Es gestiona el control de canvis en relació amb l'impacte que puguin tenir als sistemes? Justificació: Sí, es realitzen proves pilot per minimitzar els impactes.	Sí

3.	S'estableixen procediments de revisió després de fer canvis o actualitzacions? Justificació: Sí, es realitzen múltiples proves per validar el correcte funcionament.	Sí
4.	S'estableixen processos formals per a canvis en versions o funcionalitats noves per a programari de tercers? Justificació: Sí, aquesta validació és responsabilitat del partner.	Sí
5.	Es defineixen polítiques de seguretat de la informació en processos d'enginyeria de sistemes? Justificació: Sí, hi ha definida la política i està validada per l'arquitecte de sistemes.	Sí
6.	Es realitza una avaluació de riscos per a eines de desenvolupament de programari? Justificació: Sí, hi ha una presa de decisions on es tenen en compte els riscos.	Sí
7.	S'acorden els requisits de seguretat de la informació per a programari desenvolupat per tercers? Justificació: Sí, s'acorden els requisits i es duu a terme una auditoria de seguretat.	Sí
8.	Es fan proves funcionals de seguretat dels sistemes abans de la seva fase de producció? Justificació: Sí, es realitzen proves funcionals de seguretat, les quals són auditades per una empresa externa.	Sí
9.	S'estableixen protocols i proves d'acceptació de sistemes per a sistemes nous i actualitzacions? Justificació: Sí, aquests protocols i proves d'acceptació són executats en un entorn específic d'acceptació.	Sí
A14.3	**Dades de prova** Nivell maduresa actual: 80%	
1.	S'utilitzen dades de prova als assaigs o proves dels sistemes? Justificació: Sí, les dades utilitzades són dades reals distorsionades que serveixen com a dades de prova.	Sí
A15	**Relació amb proveïdors**	
A15.1	**Seguretat a la relació amb proveïdors** Nivell maduresa actual: 90%	
1.	Hi ha una política de seguretat de la informació per a proveïdors que accedeixen a actius de la informació de l'empresa? Justificació: Sí, s'ha de signar un NDA (Non-disclosure	Sí

	agreement) juntament amb un document de responsabilitat.	
2.	S'han establert requisits de seguretat de la informació en contractes amb tercers? Justificació: Sí, s'ha de signar un NDA (Non-disclosure agreement) juntament amb un document de responsabilitat.	Sí
3.	Es fixen requisits per estendre la seguretat de la informació a tota la cadena de subministrament? Justificació: Sí, s'ha de signar un NDA (Non-disclosure agreement) juntament amb un document de responsabilitat.	Sí
A15.2	**Gestió de serveis externs** Nivell maduresa actual: 80%	
1.	Es controla el compliment dels requisits establerts amb proveïdors externs? Justificació: Sí, es realitzen auditories on s'exigeixen les certificacions per part dels tercers.	Sí
2.	Es controlen els possibles impactes en la seguretat davant de canvis de serveis de proveïdors externs? Justificació: Sí, però no s'han implementat tots els controls que s'haurien de realitzar, està en procés de millora.	Sí
A16	**Gestió d'incidents de seguretat de la informació**	
A16.1	**Gestió d'incidents de seguretat de la informació i millores** Nivell maduresa actual: 80%	
1.	Es defineixen responsabilitats i procediments per respondre als incidents de la seguretat de la informació? Justificació: Sí, el responsable de seguretat és l'encarregat de realitzar les validacions de l'anàlisi post-mortem d'aquests.	Sí
2.	S'han implementat canals adequats per a la comunicació d'incidents a la seguretat de la informació? Justificació: Sí, s'han habilitat canals específics per aquestes notificacions.	Sí
3.	Es promouen i s'hagin establert canals per comunicar o identificar punts febles a la Seguretat de la Informació? Justificació: Sí, s'han habilitat canals específics per aquestes notificacions.	Sí
4.	S'ha establert un procés per gestionar els incidents a la Seguretat de la Informació? Justificació: Sí, després de cada incident es fa una anàlisi post-mortem.	Sí
5.	Hi ha mecanismes per donar resposta als esdeveniments de la Seguretat de la Informació?	Sí

	Justificació: Sí, hi ha alarmes i un procés de monitorització que està en procés de millora.	
6.	La informació que proporciona els esdeveniments a la Seguretat de la informació són tractats per prendre mesures preventives? Justificació: Sí, però es troba en una fase molt inicial.	Sí
7.	Hi ha un procés per recopilar evidències sobre els incidents en la seguretat de la informació? Justificació: Sí, després de cada incident es fa una anàlisi post-mortem.	Sí
A17	**Gestió de la continuïtat del negoci**	
A17.1	**Continuïtat de la seguretat de la informació** Nivell maduresa actual: 75%	
1.	S'ha elaborat un pla de continuïtat del negoci davant d'incidents de seguretat de la informació? Justificació: Sí, en la definició del pla director de seguretat es va contemplar el pla de continuïtat de negoci.	Sí
2.	S'han implementat les mesures de recuperació previstes al pla de Continuïtat del Negoci? Justificació: Sí, es realitzen proves per validar el pla de continuïtat de negoci.	Sí
3.	S'han verificat o provat les accions previstes al pla de Continuïtat del Negoci? Justificació: Sí, es realitzen proves per validar el pla de continuïtat de negoci.	Sí
A17.2	**Redundàncies** Nivell maduresa actual: 85%	
1.	S'ha avaluat la necessitat de redundar els actius crítics de la informació? Justificació: Sí, s'ha avaluat i implementat en els casos considerats.	Sí
A18	**Compliment**	
A18.1	**Compliment dels requisits legals i contractuals** Nivell maduresa actual: 85%	
1.	S'han identificat les legislacions aplicables sobre la protecció de dades personals i el seu compliment? -LOPD -Lleis per a comerç electrònic -Transaccions bancàries -Informació Protegida -Altres pròpies del negoci o activitat -Llei general de Telecomunicacions	Sí

	Justificació: Sí, està auditat per un departament legal extern.	
2.	Hi ha procediments implementats sobre la propietat intel·lectual? Justificació: Sí, tot treball realitzat per la companyia és propietat de l'organització.	Sí
3.	S'estableixen criteris per a classificació de registres i mesures de protecció segons nivells? Justificació: Sí, però només a certs nivells.	Sí
4.	S'estableixen mesures per a la protecció de dades personals d'acord amb la legislació vigent? Justificació: Sí, s'utilitzen eines corporatives pel desenvolupament de l'activitat.	Sí
5.	Si es fa servir el xifratge, s'estableixen controls criptogràfics d'acord amb la legislació? Justificació: Sí, es contempla dins de la política interna i s'utilitza l'eina corporativa de gestió.	Sí
A18.2	**Revisions de la seguretat de la informació** Nivell maduresa actual: 85%	
1.	Els controls de la Seguretat de la Informació són revisats per personal independent als responsables d'implementar els controls? Justificació: Sí, habitualment ho fa una empresa externa.	Sí
2.	Es revisa periòdicament el compliment de les polítiques i els controls de la Seguretat de la informació? Justificació: Sí, es revisa el compliment de les polítiques, però es troba en un procés de millora.	Sí
3.	Es fan avaluacions sobre el funcionament correcte de les mesures tècniques de protecció per a la seguretat de la informació? Justificació: Sí, mitjançant una empresa auditora externa.	Sí

10.8. Annex 8 – Avaluació de la maduresa.

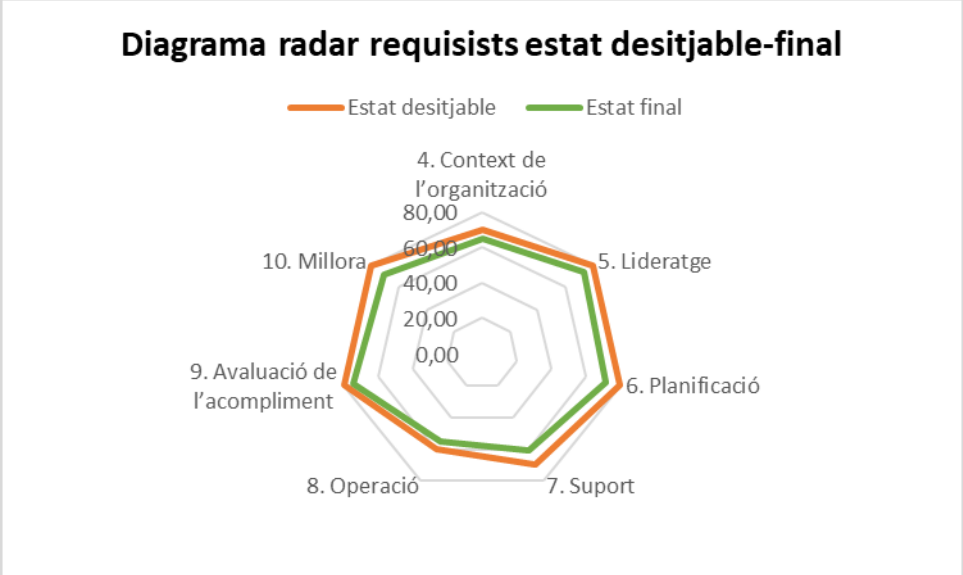
A continuació tenim disponible l'avaluació de la maduresa, on tenim representat per cada domini i control, segons els distints nivells CMM, el valor inicial, el valor final i el valor desitjable pels requisits generals de la norma ISO/IEC 27001:2013.

Nivell de compliment ISO/IEC 27001:2013					
Domini	**Control**	**Objectiu de control**	**Nivell CMM**		
			Inicial	**Final**	**Desitjable**
4. Context de l'organització			53%	65%	70%
	4.1. Comprensió de l'organització i del seu context	Determinar les qüestions pertinents que afecten la capacitat per aconseguir els resultats prevists del sistema	L2 60%	L2 68%	-
	4.2. Comprensió de les necessitats i expectatives de les parts interessades	Determinar les parts interessades i els requisits d'aquestes que són rellevants per la seguretat de la informació	L2 60%	L2 64%	-
	4.3. Determinació de l'abast del sistema de gestió de la seguretat de la informació	Definir els límits i l'aplicabilitat del sistema de gestió de la seguretat de la informació per establir l'abast	L2 50%	L2 60%	-
	4.4. Sistema de gestió de la seguretat de la informació	Establir, implementar, mantenir i millorar de manera contínua el sistema de gestió de la seguretat de la informació	L1 40%	L2 67%	-
5. Lideratge			62%	74%	80%
	5.1. Lideratge i compromís	Demostrar lideratge i compromís respecte al sistema	L2 70%	L2 79%	-
	5.2. Política	Establir una política de seguretat de la informació que sigui adequada per l'objectiu de l'organització	L2 60%	L2 75%	-
	5.3.Rols, responsabilitats i autoritats en l'organització	Assegurar-se que s'assignen i es comuniquen les responsabilitats i autoritats pels rols pertinents	L2 55%	L3 68%	-
6. Planificació			63%	72%	80%
	6.1. Accions per tractar els riscs i oportunitats	Planificar el sistema de gestió de la seguretat de la informació	L2 55%	L2 68%	-
	6.2. Objectius de	Establir els objectius de	L2	L2	-

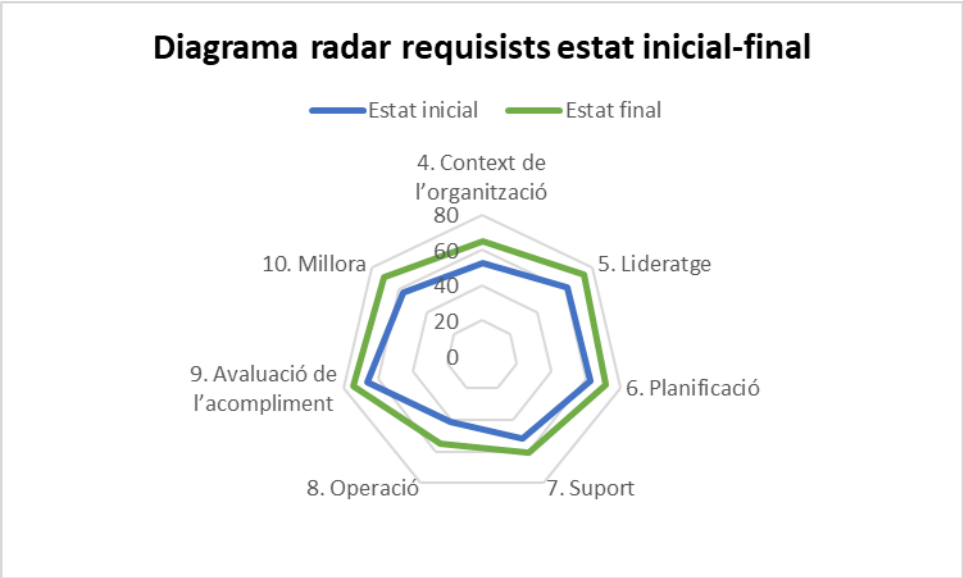
	seguretat de la informació i planificació per la consecució	seguretat de la informació en les funcions i nivells pertinents	70%	75%	
7. Suport			52%	61%	70%
	7.1. Recursos	Determinar i proporcionar els recursos necessaris per al sistema	L2 65%	L2 68%	-
	7.2. Competència	Determinar la competència necessària de les persones assegurant-se que siguin competents	L2 55%	L2 60%	-
	7.3. Conscienciació	Ser conscients de la política de seguretat, la contribució a l'eficàcia del sistema i les implicacions de no complir amb els requisits	L1 35%	L2 52%	-
	7.4. Comunicació	Determinar la necessitat de comunicacions pertinents al sistema	L1 45%	L2 56%	-
	7.5. Informació documentada	Incloure la informació documentada requerida per la norma i l'organització	L2 60%	L2 69%	-
8. Operació			42%	55%	60%
	8.1. Planificació i control operacional	Planificar, implementar i controlar els processos per complir els requisits de seguretat de la informació	L1 40%	L2 54%	-
	8.2. Apreciació dels riscs de seguretat de la informació	Determinar els riscos de seguretat de la informació a intervals planificats o quan esdevenguin modificacions importants	L1 45%	L2 59%	-
	8.3. Tractament dels riscs de seguretat de la informació	Implementar un pla de tractament de riscos de la seguretat de la informació	L1 40%	L2 52%	-
9. Avaluació de l'acompliment			67%	75%	80%
	9.1. Seguiment, mediació, anàlisi i avaluació.	Avaluar l'acompliment i l'eficàcia del sistema de gestió de la seguretat de la informació	L2 60%	L2 68%	-
	9.2. Auditoria interna	Realitzar auditories internes per aportar informació sobre el sistema	L2 70%	L2 82%	-
	9.3. Revisió per la direcció	Revisar el sistema per assegurar-se de la seva convivència, adequació i	L2 70%	L2 75%	-

		eficàcia contínua			
10. Millora			58%	71%	80%
	10.1. No conformitat i accions correctives	Reaccionar davant no conformitats, implementar accions necessàries, revisar l'eficàcia de les accions i realitzar canvis en cas que sigui necessari	L2 55%	L2 69%	-
	10.2. Millora continua	Millorar de manera contínua la idoneïtat, l'adequació i l'eficàcia del sistema	L2 60%	L2 72%	-

Un cop avaluat el nivell de compliment final, podem representar els resultats amb un diagrama radar, on podem veure el nivell de compliment per a cada un dels requisits generals de la norma i com difereixen els valors aconseguits al final del procés i els valors que s'havien assignat com a estat desitjable.



Per poder veure l'augment del nivell de compliment que s'ha produït després de la implementació dels projectes proposats, representam el següent diagrama de radar on podem comparar l'estat inicial, mesurat a l'inici del projecte a la fase 2, i l'estat final actual que s'ha aconseguit.



De la mateixa manera, disposam de l'anàlisi del nivell de compliment pels 114 controls de l'annex de la ISO/IEC 27002:2013. [6]

Nivell de compliment ISO/IEC 27002:2013					
Domini	**Control**	**Objectiu de control / Observacions**	**Nivell CMM Inicial**	**Final**	**Desitjable**
5. Polítiques de seguretat de la informació			45%	59%	70%
	5.1.1. Polítiques per la seguretat de la informació	El document s'ha de crear amb la participació de l'alta direcció, el departament de TI i seguretat.	L2 50%	L2 73%	-
	5.1.2. Revisió de les polítiques per la seguretat de la informació	S'ha de garantir un cronograma de revisió periòdica de les polítiques per la seguretat de la informació	L1 40%	L2 45%	-
6. Organització de la seguretat de la informació			57%	69%	70%
	6.1.1. Rols i responsabilitats en seguretat de la informació	S'ha de fitxar una estructura organitzativa segons les responsabilitats assignades	L2 60%	L2 84%	-
	6.1.2. Segregació de tasques	Es defineixen les responsabilitats acord amb el rol de cada treballador	L2 50%	L2 73%	-
	6.1.3. Contacte amb les autoritats	S'han de definir els canals de comunicació oficials per gestionar les diverses situacions que sorgeixin	L2 60%	L2 66%	-
	6.1.4. Contacte amb grups d'interès especial	Tenir contacte amb especialistes en la matèria per tenir major facilitat per	L2 50%	L2 57%	-

		gestionar les diverses situacions que sorgeixin			
	6.1.5. Seguretat de la informació en la gestió de projectes	S'ha de tractar la seguretat de la informació dins de la gestió de projectes	L2 60%	L2 79%	-
	6.2.1. Política de dispositius mòbils	S'han de definir polítiques per l'ús de dispositius mòbils.	L2 50%	L2 56%	-
	6.2.2. Teletreball	S'ha de definir una política i les mesures de seguretat adequades per protegir la informació tractada o emmagatzemada en els dispositius de teletreball	L2 60%	L2 69%	-
7. Seguretat relativa als recursos humans			53%	65%	75%
	7.1.1. Investigació d'antecedents	S'ha de definir una política en el procés de contractació.	L1 40%	L1 49%	-
	7.1.2. Terminis i condicions de l'empleat	S'ha de tenir definit un procés contractual establert i aplicable als càrrecs de l'organització	L2 65%	L2 77%	-
	7.2.1. Responsabilitats de gestió	Cal tenir les responsabilitats clares per la gestió	L2 70%	L2 83%	-
	7.2.2. Conscienciació, educació i capacitació en seguretat de la informació	Cal realitzar campanyes de sensibilització sobre la seguretat de la informació de manera periòdica	L2 50%	L2 69%	-
	7.2.3. Procés disciplinari	El contracte ha de tenir unes clàusules ben definides per si es dona el cas d'un procés disciplinari	L2 60%	L2 60%	-
	7.3.1. Responsabilitats davant la finalització o el canvi	Definir procediments clars per quan un treballador finalitzi o canvi el lloc de treball	L1 45%	L1 52%	-
8. Gestió d'actius			61%	73%	80%
	8.1.1. Inventari d'actius	Disposar d'un inventari d'actius indicant el responsable i la ubicació d'aquest	L2 70%	L2 82%	
	8.1.2. Propietat dels actius	Disposar d'una classificació dels actius	L2 80%	L2 86%	
	8.1.3. Ús acceptable dels actius	Tenir una política ben definida que contempli l'ús acceptable d'actius	L2 75%	L2 85%	
	8.1.4. Devolució	Tenir definit el procediment	L2	L2	

	d'actius	per realitzar la devolució d'actius dels treballadors	70%	78%	
	8.2.1. Classificació de la informació	Comptar amb una correcta classificació de la informació	L2 65%	L2 77%	
	8.2.2. Etiquetat de la informació	La classificació de la informació ha de tenir el respectiu etiquetat per tal de poder reconèixer-la	L2 70%	L2 74%	
	8.2.3. Manipulació de la informació	Definir una política per la manipulació de la informació i el tractament d'aquesta	L2 70%	L2 79%	
	8.3.1. Gestió de suports extraibles	Disposar de la informació necessària per gestionar de manera correcta tots els dispositius d'emmagatzemament extraïble	L1 30%	L1 44%	
	8.3.2. Eliminació de suports	Assegurar-se que els dispositius s'eliminien adequadament minimitzant el risc de fuga d'informació	L2 50%	L2 69%	
	8.3.3. Suports físics en trànsit	Realitzar un seguiment dels suports físics en trànsit per assegurar-se del correcte ús d'aquests	L1 40%	L2 52%	
9. Control d'accés			68%	76%	90%
	9.1.1. Política de control d'accés	Implementació de controls físics i lògics per millorar l'accés a la informació	L2 65%	L2 69%	-
	9.1.2. Accés a les xarxes i als serveis de xarxa	Disposar de controls d'accés a la xarxa i als serveis d'aquesta	L2 70%	L2 88%	-
	9.2.1. Registre i baixa d'usuari	Garantir el correcte procediment d'altes i baixes dels usuaris	L2 70%	L2 79%	-
	9.2.2. Provisió d'accés de l'usuari	Garantir una correcta assignació i revocació dels drets d'accés de l'usuari	L2 60%	L2 75%	-
	9.2.3. Gestió de privilegis d'accés	Assignació i ús de privilegis d'accés restringida i controlada	L2 80%	L2 86%	-
	9.2.4. Gestió de la informació secreta d'autenticació dels usuaris	Control formal de l'assignació de la informació secreta o confidencial	L2 60%	L2 79%	-
	9.2.5. Revisió dels drets d'accés d'usuari	Revisar els drets d'accés dels usuaris de manera regular	L2 60%	L2 63%	-

	9.2.6. Retirada o reassignació dels drets d'accés	Definir un control sobre l'agregació o retirada dels drets d'accés	L1 40%	L2 64%	-
	9.3.1. Ús de la informació secreta d'autenticació	Fitxar el control i la política per la gestió de contrasenyes	L2 70%	L2 79%	-
	9.4.1. Restricció d'accés a la informació	Definir controls per restringir l'accés a la informació	L2 80%	L2 88%	-
	9.4.2. Procediments segurs d'inici de sessió	Controlar els procediments d'inici de sessió	L2 70%	L2 75%	-
	9.4.3. Sistema de gestió de contrasenyes	Disposar de procediments clars per la gestió de contrasenyes	L2 60%	L2 62%	-
	9.4.4. Ús d'utilitats amb privilegis del sistema	Restringir i controlar l'ús d'utilitats que puguin invalidar els controls del sistema	L2 70%	L2 73%	-
	9.4.5. Control d'accés al codi font dels programes	Restringir l'accés al codi font dels programes	L2 80%	L2 80%	-
10. Criptografia			55%	62%	80%
	10.1.1. Política d'ús dels controls criptogràfics	Establir controls criptogràfics per la protecció de la informació de l'organització	L2 60%	L2 63%	-
	10.1.2. Gestió de claus	Disposar d'una política per controlar l'ús, la protecció i la durada de les claus de xifratge	L2 50%	L2 61%	-
11. Seguretat física i de l'entorn			68%	76%	80%
	11.1.1. Perímetre de seguretat física	Establir perímetres d'accés restringits i de lliure accés	L2 80%	L2 88%	-
	11.1.2. Controls físics d'entrada	Àrees definides mitjançant controls físics d'entrada adients	L3 90%	L3 90%	-
	11.1.3. Seguretat d'oficines, despatxos i recursos	Implementació de controls i protocols d'accés *Obs.: S'han detectat aspectes de millora en la seguretat física aplicada a l'accés de les oficines centrals	L2 80%	L2 83%	-
	11.1.4. Protecció contra les amenaces externes i ambientals	Garantir la protecció contra les amenaces	L2 70%	L3 92%	-
	11.1.5. El treball en	Dissenyar i implementar	L2	L2	-

	àrees segures	procediments per garantir el treball en àrees segures	75%	78%	
	11.1.6. Àrees de carrega i descarrega	Implementar controls els punts d'accés	L2 80%	L2 87%	-
	11.2.1. Emplaçament i protecció d'equips	Definir controls per la protecció i emplaçament dels equips	L2 50%	L2 66%	-
	11.2.2. Instal·lacions de subministrament	Fitxar controls per la protecció de les instal·lacions contra falles d'alimentació	L2 65%	L2 74%	-
	11.2.3. Seguretat del cablejat	Garantir la seguretat física del cablejat	L2 70%	L2 77%	-
	11.2.4. Manteniment dels equips	Definir programes de manteniment dels equips per assegurar la seva disponibilitat i integritat	L2 60%	L2 79%	-
	11.2.5. Retirada de materials propietat de l'empresa	Implementar el control d'actius que pertanyen a l'organització i s'utilitzen fora d'ella	L2 50%	L2 63%	-
	11.2.6. Seguretat dels equips fora de les instal·lacions	Aplicar mesures de seguretat pels equips que es troben fora de les instal·lacions de l'organització	L2 50%	L2 72%	-
	11.2.7. Reutilització o eliminació segura dels equips	Verificar que s'ha eliminat la informació confidencial dels equips de manera segura abans d'eliminar-los	L2 60%	L2 75%	-
	11.2.8. Equip d'usuari desatengut	Comprovar que els equips desatenguts tenen la protecció adequada	L2 50%	L2 54%	-
	11.2.9. Política de lloc de treball buit i pantalla neta	Realitzar campanyes per conscienciar als treballadors de la importància de tenir el lloc de treball en condicions	L2 60%	L2 65%	-
12. Seguretat de les operadores			67%	78%	80%
	12.1.1. Documentació de procediments de les operacions	Definir procediments d'operació i registre formal	L2 70%	L2 79%	-
	12.1.2. Gestió dels canvis	Establir procediments de control i gestió als canvis	L2 50%	L2 78%	-
	12.1.3. Gestió de les capacitats	Supervisar i ajustar la utilització de recursos per garantir el rendiment	L2 60%	L2 83%	-

		requerit del sistema			
	12.1.4. Separació dels recursos de desenvolupament, prova i operació	Garantir i implementar zones segures de desenvolupament per la posterior producció	L2 70%	L2 82%	-
	12.2.1. Controls contra el codi maliciós	Definir estratègies i eines per controlar el codi maliciós	L2 70%	L2 86%	-
	12.3.1. Copies de seguretat de la informació	Establir processos de còpies de seguretat de la informació, del software i del sistema	L2 80%	L2 85%	-
	12.4.1. Registre d'esdeveniments	Registrar i gestionar els esdeveniments que es realitzen per les diferents activitats	L2 80%	L2 85%	-
	12.4.2. Protecció de la informació del registre	Protegir els registres de la informació contra manipulacions indegudes i accessos no autoritzats	L2 70%	L2 83%	-
	12.4.3. Registres d'administració i operació	Definir registres per tal de protegir i revisar les activitats dels usuaris periòdicament	L2 65%	L2 80%	-
	12.4.4. Sincronització del rellotge	Controlar formalment la sincronització de rellotges de l'organització	L2 50%	L2 77%	-
	12.5.1. Instal·lació del software en explotació	Implementar procediments per controlar la instal·lació del software en explotació	L2 65%	L2 67%	-
	12.6.1. Gestió de les vulnerabilitats tècniques	Controlar la gestió de les vulnerabilitats tècniques que es detectin	L2 60%	L2 69%	-
	12.6.2. Restricció en la instal·lació del software	Garantir el control de la instal·lació del software	L2 50%	L2 64%	-
	12.7.1. Controls d'auditoria de sistemes d'informació	Fitxar controls d'auditoria pels sistemes d'informació	L2 70%	L2 75%	-
13. Seguretat de les comunicacions			58%	73%	90%
	13.1.1. Controls de xarxa	Administrar i gestionar les xarxes per protegir a informació dels sistemes	L2 65%	L2 79%	-
	13.1.2. Seguretat dels serveis de xarxa	Identificar i implementar mecanismes de seguretat	L2 60%	L2 86%	-
	13.1.3. Segregació en xarxa	Segregar en distintes xarxes els grups de serveis de la informació	L1 40%	L2 66%	-

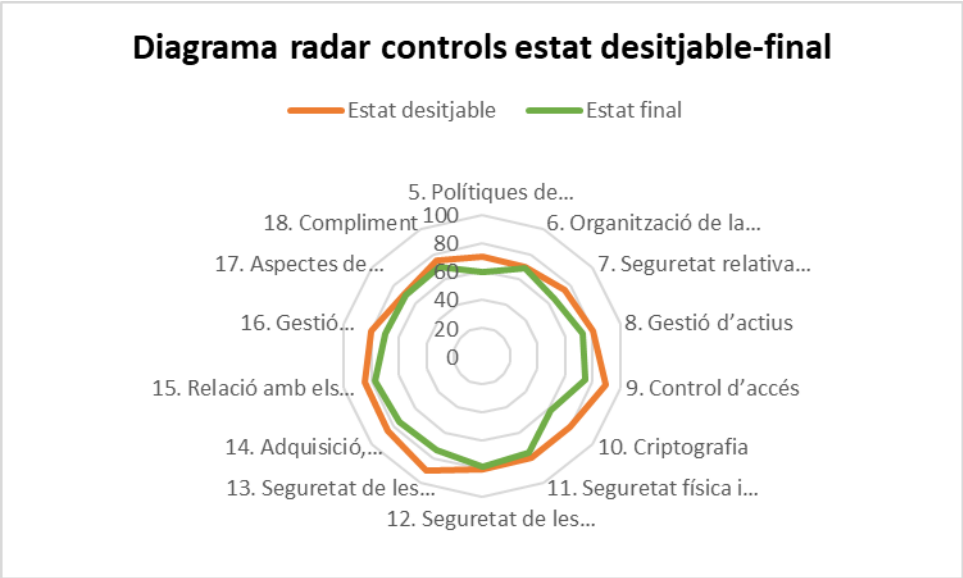
	13.2.1. Polítiques i procediments d'intercanvi d'informació	Establir polítiques per l'intercanvi d'informació	L2 50%	L2 69%	-
	13.2.2. Acords d'intercanvi d'informació	Garantir acords per la transferència segura de la informació	L2 50%	L2 55%	-
	13.2.3. Missatgeria electrònica	Implementar controls i polítiques d'ús de missatgeria electrònica	L2 60%	L2 67%	-
	13.2.4. Acords de confidencialitat o no revelació	Implementar acords de confidencialitat per protegir la informació	L2 85%	L2 88%	-
14. Adquisició, desenvolupament i manteniment			67%	75%	85%
	14.1.1. Anàlisi de requisits i especificacions de seguretat de la informació	Analitzar les vulnerabilitats dels sistemes d'informació per tal de fitxar mesures sobre aquests	L2 60%	L2 74%	-
	14.1.2. Assegurar els serveis d'aplicacions en xarxes públiques	Implementar solucions de seguretat per poder controlar l'accés als serveis d'informació	L2 75%	L2 83%	-
	14.1.3. Protecció de les transaccions de servidors d'aplicacions	Fitxar el control per la protecció de transaccions en xarxa	L2 70%	L2 86%	-
	14.2.1. Política de desenvolupament segur	Establir i aplicar regles dins l'organització pel desenvolupament d'aplicacions i sistemes	L2 70%	L2 79%	-
	14.2.2. Procediment de control de canvis en els sistemes	Definir un control per la gestió dels canvis	L2 70%	L2 82%	-
	14.2.3. Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu	Fitxar una revisió i proves de les aplicacions per garantir la seguretat de la informació	L2 70%	L2 70%	-
	14.2.4. Restriccions als canvis en els paquets de software	Garantir que no es produiran modificacions dels paquets de software entregats per tercers	L1 40%	L1 49%	-
	14.2.5. Principis d'enginyeria de sistemes segurs	Implementar mesures per assegurar-se la protecció dels sistemes	L2 60%	L2 71%	-
	14.2.6. Entorn de desenvolupament segur	Assegurar l'entorn de desenvolupament	L2 70%	L2 78%	-
	14.2.7.	Supervisar i controlar el	L2	L2	-

	Externalització del desenvolupament de software	desenvolupament del software de l'organització	70%	88%	
	14.2.8. Proves funcionals de seguretat de sistemes	Realitzar proves de seguretat durant el desenvolupament	L2 70%	L2 77%	-
	14.2.9. Proves d'acceptació de sistemes	Establir programes de prova d'acceptació i criteris relacionats amb els sistemes d'informació	L2 70%	L2 74%	-
	14.3.1. Protecció de les dades de prova	Seleccionar, protegir i controlar les dades de prova	L2 60%	L2 63%	-
15. Relació amb els proveïdors			70%	78%	85%
	15.1.1. Política de seguretat de la informació en les relacions amb els proveïdors	Implementar la política de seguretat de la informació per mitigar els riscos associats amb l'accés als actius del proveïdor	L2 70%	L2 85%	-
	15.1.2. Requisits de seguretat en contractes amb tercers	Fitxar els requisits relacionats amb la seguretat de la informació en contractes amb proveïdors	L2 70%	L2 79%	-
	15.1.3. Cadena de subministrament de tecnologia de la informació i de les comunicadores	Implementar un control per garantir la cadena de subministrament en tecnologies de la informació	L2 70%	L2 77%	-
	15.2.1. Control i revisió de la provisió dels serveis del proveïdor	Implementar controls per la supervisió de contractes amb tercers	L2 70%	L2 75%	-
	15.2.2. Gestió de canvis en la provisió del servei del proveïdor	Implementar control dels canvis als serveis de tercers	L2 70%	L2 75%	-
16. Gestió d'incidents de seguretat de la informació			61%	70%	80%
	16.1.1. Responsabilitats i procediments	Assignar les responsabilitats i els procediments per la gestió dels incidents	L2 60%	L2 78%	-
	16.1.2. Notificació dels esdeveniments de seguretat de la informació	Determinar el control per notificar i prendre les mesures respectives	L2 60%	L2 68%	-
	16.1.3. Notificació de punts dèbils de la seguretat	Realitzar controls per l'establiment de punts dèbils de seguretat	L2 70%	L2 73%	-

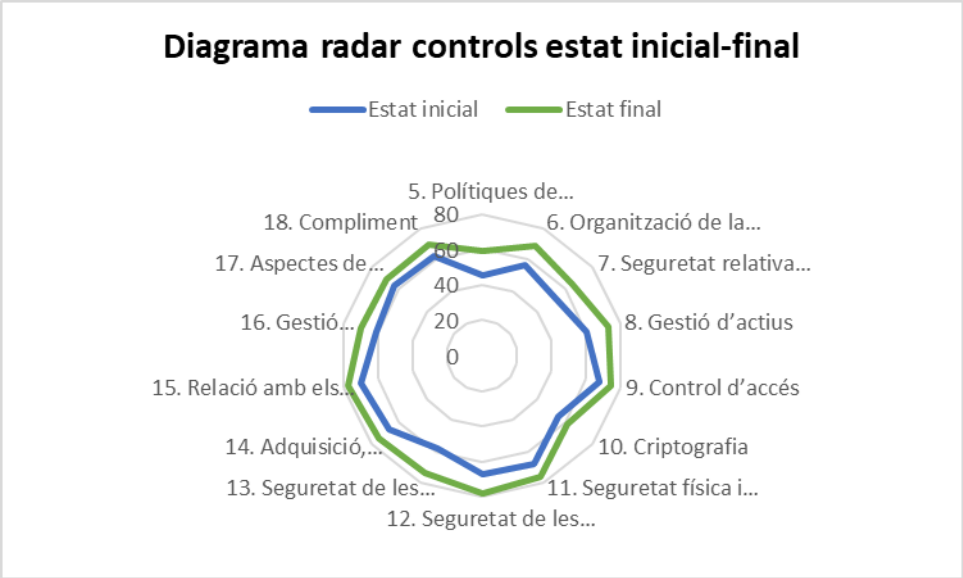
	16.1.4. Avaluació i decisió sobre els esdeveniments de seguretat d'informació	Fitxar el control per l'avaluació d'un esdeveniment i prendre les pertinents mesures	L2 60%	L2 65%	-
	16.1.5. Resposta a incidents de seguretat de la informació	Fitxar un procediment per donar resposta als incidents que esdevenguin relacionats amb la seguretat de la informació	L2 60%	L2 73%	-
	16.1.6. Aprenentatge dels incidents de seguretat de la informació	Tenir un control dels incidents per tal de reduir l'impacte en incidents futurs	L2 50%	L2 64%	-
	16.1.7. Recopilació d'evidències	Definir i aplicar procediments per identificar, adquirir i perseverar la informació que pugui servir d'evidència	L2 60%	L2 65%	-
17. Aspectes de seguretat de la informació per la gestió de la continuïtat del negoci			63%	69%	70%
	17.1.1. Planificació de la continuïtat de la seguretat de la informació	Tenir definit el pla de continuïtat de negoci	L2 60%	L2 75%	-
	17.1.2. Implementar la continuïtat de la seguretat de la informació	Implementar els plans de continuïtat de la seguretat de la informació	L2 60%	L2 68%	-
	17.1.3. Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació	Definir un cronograma de proves per assegurar la continuïtat del pla de negoci	L2 50%	L2 62%	-
	17.2.1. Disponibilitat dels recursos de tractament de la informació	Implementar els recursos de tractament de la informació per tal de satisfer els requisits de disponibilitat	L2 70%	L2 73%	-
18. Compliment			63%	70%	75%
	18.1.1. Identificació de la legislació aplicable dels requisits contractuals	Revisar les condicions i obligacions legals per evitar un incompliment	L2 70%	L2 75%	-
	18.1.2. Drets de propietat intel·lectual (DPI)	Implementar procediments per garantir el compliment dels requisits legals,	L2 65%	L2 65%	-

		reguladors i contractuals			
	18.1.3. Protecció dels registres de l'organització	Implementació d'acords de confidencialitat per estar protegits contra la pèrdua, destrucció, manipulació o accessos no autoritzats	L2 70%	L2 70%	-
	18.1.4. Protecció i privacitat de la informació de caràcter personal	Classificar la informació segons requereixi la legislació i la reglamentació	L2 60%	L2 70%	-
	18.1.5. Regulació dels controls criptogràfics	Implementar controls de regulació criptogràfica	L2 60%	L2 65%	-
	18.2.1. Revisió independent de la seguretat de la informació	Realitzar una revisió independent planificada o quan succeeixin canvis significatius en la implementació	L2 60%	L2 65%	-
	18.2.2. Compliment de les polítiques i normes de seguretat	Implementar auditories internes de compliment per verificar que es compleixen correctament les polítiques i les normes	L2 60%	L2 65%	-
	18.2.3. Comprovació del compliment tècnic	Revisar i contrastar els controls mitjançant les auditories realitzades	L2 60%	L2 65%	-

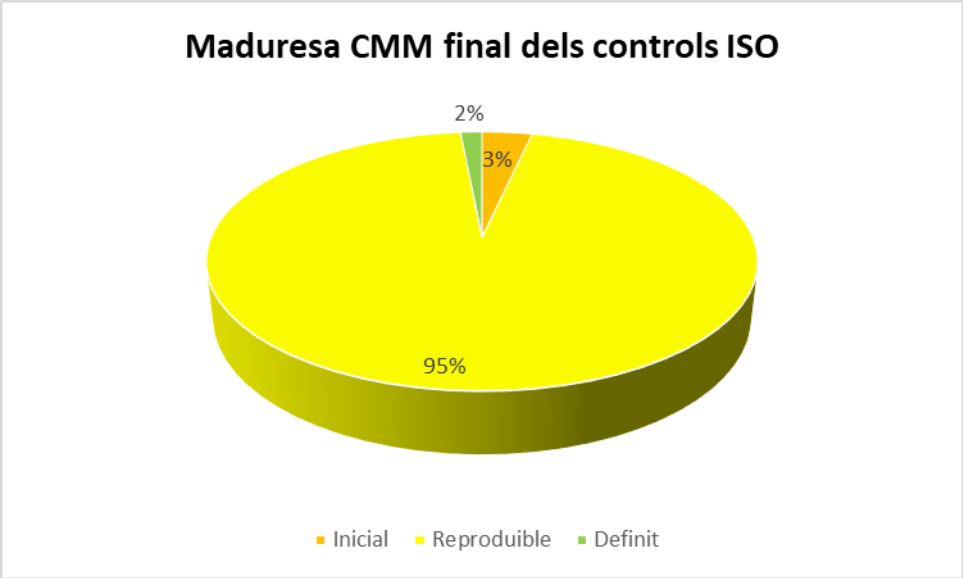
Quan ja hem finalitzat l'anàlisi del nivell de compliment dels controls de l'annex de la norma, podem representar els resultats obtinguts amb un diagrama radar, on podem veure el nivell de compliment per a cada un dels controls d i com difereixen els valors al final del procés i els valors que s'havien assignat com a estat desitjable.



També podem veure la millora que s'ha produït del nivell de compliment en els controls després de la implementació dels projectes proposats, en comparació amb l'estat inicial.



A més a més, amb els resultats obtinguts podem generar un altre diagrama per tal de veure en termes generals el nivell de maduresa dels controls de la ISO/IEC 27001:2013 segons l'escala definida pel CMM, on tenim un 2% de maduresa de nivell L1 "Inicial/Ad-hoc", un 95% de maduresa de nivell L2 "Reproduïble però intuïtiu" i un 3% de maduresa de nivell L3 "Procés definit".



10.9. Annex 9 – Informe d'auditoria

A continuació es presenta l'informe d'auditoria resultant:

<table>
<tr><th colspan="2">Informe auditoria interna
(Nom de l'empresa – logotip de l'empresa)</th></tr>
<tr><td>Versió: VER-001</td><td>Codi: 2022-06-01</td></tr>
<tr><td>Data: Juny 2022</td><td>Localització: Oficines centrals de l'empresa, Palma - Mallorca</td></tr>
<tr><td colspan="2">Equip auditor: Empresa auditoria interna en col·laboració de personal extern de l'organització</td></tr>
<tr><td colspan="2">Abast de l'auditoria: L'abast del Pla Director de Seguretat (PDS) és l'oficina central de la divisió hotelera de l'empresa.</td></tr>
<tr><td colspan="2">Objectius de l'auditoria: Avaluar el nivell actual de maduresa en termes de ciberseguretat de l'empresa, identificar i documentar un mapa de riscos per la companyia, definir les iniciatives en matèria de seguretat de la informació que seran necessàries implementar sobre l'organització per aconseguir la situació objectiu, on s'establirà un full de ruta de projectes a curt, mitjà i llarg termini.

Revisió dels dominis i controls de seguretat englobats a la normativa ISO/IEC 27001:2013 per tal de determinar el nivell de compliment de la norma per part de l'empresa i detectar les no conformitats d'aquesta.</td></tr>
<tr><td colspan="2">Activitats desenvolupades:
Revisió de l'estat de seguretat de la informació
Identificació de les debilitats en els processos de seguretat implementats.
Comprensió dels processos de negoci de l'empresa.
Revisió del nivell de maduresa dels processos de ciberseguretat existents respecte a la ISO 27001. Per això es realitzen entrevistes i es revisa la documentació existent per avaluar els següents aspectes:
Política de seguretat de la informació.
Rols i funcions en seguretat de la informació.
Anàlisis de risc de continuïtat, Pla de Continuïtat del Negoci.
Procediment de gestió d'accés físic.
Procediment de gestió d'usuaris.
Classificació de la informació.
Normes bàsiques de seguretat en l'ús dels recursos de la informació.
Clàusules en la selecció i contractació del personal.
Guies de bastionat.
Detecció de vulnerabilitats.
Guies de desenvolupament segur.
Processos i procediments de gestió dels canvis.
Gestió d'incidents de seguretat.</td></tr>
</table>

- Protecció enfront del malware.

Resultats auditoria

- **NC-01**: No existeix un cos normatiu de seguretat de la informació com a tal més enllà dels procediments operatius existents, creats a nivell de departament.
  - Domini ISO: A.5. Polítiques de seguretat.
  - Categoria: No conformitat menor.

- **NC-02**: No existeix una política de gestió de dispositius mòbils, malgrat s'apliquin mesures per la protecció de l'ús d'aquests. Seria recomanable la seva definició, compartir-la amb els usuaris i aplicar les mesures organitzatives i tècniques necessàries perquè aquestes es compleixin.
  - Domini ISO: A.6. Organització de seguretat de la informació.
  - Categoria: No conformitat menor.

- **NC-03**: No existeix una política que defineixi la revisió dels drets d'accés dels treballadors, malgrat que es duguin a terme accions per evitar que el personal no autoritzat tengui accés a informació confidencial de l'organització, el procés de gestió d'usuaris hauria d'estar suportat per una plataforma que garantís la confidencialitat de la informació.
  - Domini ISO: A.9. Control d'accés.
  - Categoria: No conformitat menor.

- **NC-04**: No existeix una eina de gestió de contrasenyes. Les contrasenyes d'accés a les diferents plataformes són gestionades de manera aïllada per cadascú i la seva gestió es duu a terme manualment pel personal responsable de l'entorn.
  - Domini ISO: A.9. Control d'accés.
  - Categoria: No conformitat menor.

- **NC-05**: No existeix una política que defineixi els controls a aplicar per la protecció del treball en àrees segures.
  - Domini ISO: A.11. Seguretat física i de l'entorn.
  - Categoria: No conformitat menor.

- **NC-06**: No existeix una política que reculli les restriccions que s'haurien d'aplicar sobre els paquets de software utilitzats per l'organització.
  - Domini ISO: A.14. Adquisició, desenvolupament i manteniment de sistemes.
  - Categoria: No conformitat menor.

- **M-01**: No existeix una política de gestió d'accés com a tal, des de l'organització s'apliquen mesures de protecció contra l'accés indegut als distints entorns.
  - Domini ISO: A.9. Control d'accés
  - Categoria: Millora.

- **M-02**: Els procediments existents sobre la configuració segura de les

connexions als SSII de l'organització no estan formalitzats. Seria recomanable disposar d'un cos normatiu en matèria de ciberseguretat que reguli la configuració de les connexions als SSII.
    - Domini ISO: A.9. Control d'accés
    - Categoria: Millora

- **M-03**: No existeix una política d'ús de controls criptogràfics. Els controls aplicats depenen de l'entorn i la decisió del responsable d'aquest. Seria recomanable definir una política que reguli i estandaritzi l'ús de controls criptogràfics.
    - Domini ISO: A.10. Criptografia
    - Categoria: Millora

- **M-04**: No existeix una política de gestió de claus de xifratge, sinó que són actualitzades, normalment, baix necessitat. Seria recomanable definir una política per controlar i uniformitzar la gestió de claus de xifratge.
    - Domini ISO: A.10. Criptografia
    - Categoria: Millora

- **M-05**: S'han detectat aspectes a millorar en la seguretat física aplicada a l'accés de les oficines centrals. Seria recomanable augmentar el nivell de seguretat mitjançant l'ús de targetes identificatives, empremta dactilar o reconeixement facial.
    - Domini ISO: A.11. Seguretat física i de l'entorn
    - Categoria: Millora

- **M-06**: No existeix una política d'escriptori i pantalla neta. Es recomana acompanyar la definició d'aquesta política amb la implementació de mesures que recordin als usuaris que és d'obligat compliment.
    - Domini ISO: A.11. Seguretat física i de l'entorn
    - Categoria: Millora

- **M-07**: No es disposa d'una eina per la monitorització i l'anàlisi dels registres. Tot i això, es recullen els logs d'activitat sobre alguns SSII crítics. Es recomana disposar d'una eina de monitorització i anàlisi per tal de millorar la gestió dels registres.
    - Domini ISO: A.12. Seguretat de les comunicacions.
    - Categoria: Millora

- **M-08**: No existeix un procediment de resposta ni de report d'incidències de seguretat ocorregudes en l'organització. Aquests reports es realitzen baix la necessitat o com a resultat d'una anàlisi en concret. Es recomana implementar un procediment de resposta i report d'incidents.
    - Domini ISO: A.16. Gestió d'incidents de seguretat de la informació
    - Categoria: Millora

- **M-09**: No existeix un procediment de gestió dels drets de la propietat intel·lectual, però en qualsevol cas les mesures de protecció de la

informació de l'organització estan protegides segons les directrius de seguretat de la informació.
    - Domini ISO: A.18. Compliment
    - Categoria: Millora

Observacions:

- **OBS-01**: Per alguns casos en concret hi pot haver acords de confidencialitat, però en general no existeix cap política o acord que reflecteixi exactament les conseqüències que suposaria no fer un bon ús de la informació.
    - Domini ISO: A.7. Seguretat relativa als recursos humans
    - Categoria: Observació

- **OBS-02**: L'accés als entorns amb permisos d'administrador es controlen pel responsable de cada entorn. Malgrat que el procés no estigui formalitzat ni unificat, només es concedeixen els permisos al personal qualificat i preparat per a tal fi.
    - Domini ISO: A.9. Control d'accés.
    - Categoria: Observació.

- **OBS-03**: Malgrat el procés de gestió d'accés al codi font no estigui formalitzat ni sigui uniforme per tots els entorns, només els usuaris administradors del sistema que estiguin autoritzats tenen accés a ell.
    - Domini ISO: A.9. Control d'accés.
    - Categoria: Observació.

- **OBS-04**: L'accés als equips està protegit únicament amb un identificador d'usuari i contrasenya. No s'ha aplicat cap restricció addicional com, per exemple, el doble factor d'autenticació.
    - Domini ISO: A.11. Seguretat física i de l'entorn.
    - Categoria: Observació.

- **OBS-05**: No existeix un cos normatiu ni procediments que reflecteixin els processos operatius que puguin tenir afectació a la seguretat de la informació de l'empresa.
    - Domini ISO: A.12. Seguretat en les operacions
    - Categoria: Observació.

- **OBS-06**: La formalització d'acords en transferències d'informació no és una pràctica habitual, ni d'interns ni de tercers.
    - Domini ISO: A.13. Seguretat de les comunicacions.
    - Categoria: Observació.

- **OBS-07**: Malgrat la no existència d'un procés de revisió de compliment i anàlisi de polítiques aplicables, l'organització està al corrent de les normes i els requeriments contractuals aplicables en matèria de ciberseguretat.
    - Domini ISO: A.18. Compliment
    - Categoria: Observació.

- **OBS-08**: Malgrat que no estigui regit per cap política de l'empresa, periòdicament es realitza una anàlisi del nivell de maduresa de l'organització en seguretat de la informació.
    - Domini ISO: A.18. Compliment
    - Categoria: Observació

Conclusions:

Com es pot observar amb el desenvolupament d'aquest projecte, el nivell de compliment de la seguretat de la informació de l'organització ha anat millorant progressivament, tot i que encara no s'han aconseguit els nivells proposats com a objectius, però sí que s'ha notat un augment del compliment i un augment significatiu en la maduresa de la seguretat de la informació.

A més a més, com a conclusió d'aquesta auditoria hem detectat i definit vàries no conformitats menors, les quals no posen en risc l'activitat del sistema malgrat que incompleixin alguns dels requisits o controls estudiats, i vàries millores que es podrien fer. També s'han aportat una sèrie d'observacions que s'han vist i considerat important mencionar. Cal destacar que no s'ha identificat cap no conformitat major, el que és molt important, ja que d'aquesta manera l'organització pot seguir el curs de la seva activitat, no es posa en risc la integritat del sistema. Per les no conformitats esmentades, serà necessari que l'organització estableixi i documenti les accions correctives pertinents.

Nom de l'auditor / DNI / Firma

Margalida Pau Canet Urrea (Firma)
4153xxxxF