Pla director de seguretat de l'Organització

Nom Estudiant: Eugeni Platas Sirvent

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: Maig de 2022

FITXA DEL TREBALL FINAL

Títol del treball:	*Pla director de seguretat de l'Organització*
Nom de l'autor:	*Eugeni Platas Sirvent*
Nom del consultor/a:	*José Luis Dürsteler Esteban*
Nom del PRA:	*Carles Garrigues Olivella*
Data de lliurament (mm/aaaa):	*05/2022*
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	*Seguretat, ISO, Gestió*

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

La creixent rellevància de les tecnologies de la informació per a la consecució dels objectius de negoci de l'empresa analitzada fa que augmenti cada cop més la importància de la seguretat de la informació.

El present treball planteja l'establiment de les bases per a la realització del pla director de seguretat de l'Organització, perseguint com a objectiu final la millora de la seguretat de la mateixa i possibilitant la implantació d'un sistema de gestió en procés de millora contínua.

Primerament, es determina quina és la situació actual de l'Organització des del punt de vista de la seguretat, en base a allò definit a l'estàndard internacional ISO/IEC 27001 i als controls ISO/IEC 27002. Com a part de l'estudi, es realitza també un anàlisi de riscos, basat en la metodologia Magerit.

Un cop analitzada la situació inicial i identificats els possibles punts de millora, es proposen un conjunt de projectes amb la finalitat d'augmentar el nivell de seguretat de l'empresa. Es compara, ara, l'estat inicial amb l'estat després de l'aplicació de les mesures proposades.

Finalment, i suposant una implementació completa dels projectes proposats, es realitza una auditoria de seguretat, en la que s'avalua el compliment de la norma ISO/IEC 27001,

dels controls ISO/IEC 27002 i dels objectius de seguretat definits. A més, s'identifiquen les no-conformitats existents, així com es fan recomanacions de possibles millores.

Abstract (in English, 250 words or less):

Information technologies are becoming more and more important as a critical factor for achieving the business objectives of the analyzed company. This, in turn, leads to an increase of the importance of information security.

This thesis aims to lay the foundations of an information security master plan for the organization, by pursuing the final goal of improving its security level and allowing the implementation of a continuously improved information security management system.

First, we need to determine what the actual security level of the organization is, by using the international standards ISO/IEC 27001 and ISO/IEC 27002. As part of the initial evaluation, we also perform a risk analysis, following the Magerit methodology.

Once the initial situation has been determined and we have identified possible aspects to be improved, a set of projects is proposed in order to increase the organization security level.

Finally, and considering the successful adoption and implementation of the measures proposed before, we conduct a security audit. As part of this audit, we evaluate what the compliance level with the standards ISO/IEC 27001 and ISO/IEC 27002 is, as well as the degree of achievement of the defined security goals. Furthermore, the identified non-conformities are listed and some recommendations are made.

Índex

1. Introducció....13
1.1 Context i justificació del Treball....13
1.2 Objectius del Treball....13
1.3 Enfocament i mètode seguit....14
1.4 Planificació del Treball....14
1.5 Breu sumari de productes obtinguts....16
1.6 Breu descripció dels altres capítols de la memòria....16
2. Descripció de l'Organització....18
3. Abast del pla director de seguretat....20
4. Anàlisi de compliment inicial....21
4.1 Anàlisi de compliment inicial de la norma ISO/IEC 27001....21
4.2 Anàlisi de compliment inicial dels controls ISO/IEC 27002....27
5. Esquema documental ISO/IEC 27001....35
5.1 Política de Seguretat....35
5.2 Procediment d'Auditories Internes....35
5.3 Gestió d'Indicadors....35
5.4 Procediment de Revisió per Direcció....36
5.5 Gestió de Rols i Responsabilitats....36
5.6 Metodologia d'Anàlisi de Riscos....36
5.7 Declaració d'Aplicabilitat....36
6. Anàlisi de riscos....37
6.1 Abast....37
6.2 Inventari d'actius....37
6.3 Taula de valoracions....41
6.4 Anàlisi d'amenaces....43
6.5 Avaluacions d'impacte i probabilitats (risc)....54
7. Proposta de projectes....87
7.1 Projecte 1: Campanyes de difusió i conscienciació sobre seguretat de la informació a l'Organització....88
7.1.1 Fases del projecte....88
7.1.2 Millora del risc....91
7.1.3 Millora del compliment de la norma ISO/IEC 27001....92
7.1.4 Millora del compliment dels controls ISO/IEC 27002....93
7.2 Projecte 2: Implementació i gestió d'indicadors dels controls de seguretat....94
7.2.1 Fases del projecte....95
7.2.2 Millora del risc....97
7.2.3 Millora del compliment de la norma ISO/IEC 27001....98
7.2.4 Millora del compliment dels controls ISO/IEC 27002....98
7.3 Projecte 3: Establiment de revisions periòdiques: de la direcció, auditories internes i auditories externes....99
7.3.1 Fases del projecte....100
7.3.2 Millora del risc....103
7.3.3 Millora del compliment de la norma ISO/IEC 27001....103
7.3.4 Millora del compliment dels controls ISO/IEC 27002....105
7.4 Projecte 4: Adopció de *Security by Design* als processos de l'Organització....107
7.4.1 Fases del projecte....107

7.4.2 Millora del risc....109
7.4.3 Millora del compliment de la norma ISO/IEC 27001....111
7.4.4 Millora del compliment dels controls ISO/IEC 27002....112
7.5 Millores intrínseques (MI) per la realització del pla director de seguretat de l'Organització 113
7.5.1 Millora del risc....113
7.5.2 Millora del compliment de la norma ISO/IEC 27001....114
7.5.3 Millora del compliment dels controls ISO/IEC 27002....117
7.6 Reducció dels riscos de l'Organització després dels projectes....119
7.7 Evolució del compliment de la norma ISO/IEC 27001 després dels projectes....121
7.8 Evolució del compliment dels controls ISO/IEC 27002 després dels projectes....126
8. Auditoria de compliment de la ISO/IEC 27002:2013....134
9. Conclusions....136
10. Glossari....137
11. Bibliografia....138
12. Annex I: Política de Seguretat de la Informació....141
12.1 Necessitat de la política de seguretat....142
12.2 Abast....143
12.3 Objectius de seguretat....144
12.4 Marc regulador....145
12.5 Rols i responsabilitats....146
12.5.1 Cap de seguretat o *Chief information security officer* (CISO)....146
12.5.2 Cap del departament de les tecnologies d'informació o *IT Manager*....146
12.5.3 El proveïdor de servei o *Service provider*....146
12.5.4 Director del centre de l'Organització....147
12.5.5 Treballadors....147
12.6 Declaracions de la política....148
12.6.1 Polítiques de seguretat de la informació....148
12.6.2 Organització de la seguretat de la informació....149
12.6.3 Seguretat en els recursos humans....149
12.6.4 Gestió d'actius....149
12.6.5 Control d'accés....150
12.6.6 Criptografia....150
12.6.7 Seguretat física i de l'entorn....150
12.6.8 Seguretat a les operacions....151
12.6.9 Seguretat a les comunicacions....151
12.6.10 Adquisició, desenvolupament i manteniment de sistemes d'informació....152
12.6.11 Relació amb proveïdors....152
12.6.12 Gestió d'incidents de seguretat de la informació....152
12.6.13 Gestió de la continuïtat del negoci....153
12.6.14 Compliment....153
12.7 Tractament de desviacions i excepcions....154
13. Annex II: Procediment d'Auditories Internes....155
13.1 Introducció....156
13.2 Abast....157
13.3 Procediment d'auditories internes....158
13.3.1 Programació d'auditories internes....158
13.3.2 Responsable de l'auditoria interna....159

13.3.3 Model d'informe d'auditoria....159
14. Annex III: Gestió d'Indicadors....161
14.1 Introducció....162
14.2 Abast....163
14.3 Estructura de l'indicador....164
14.4 Monitoratge dels indicadors....165
14.4.1 Mètodes de seguiment, mesurament, anàlisi i avaluació....165
14.4.2 Quan i qui realitza el seguiment i el mesurament....166
14.4.3 Quan i qui realitza l'anàlisi i l'avaluació....166
14.5 Indicadors dels controls implementats a l'Organització....167
15. Annex IV: Procediment de Revisió per Direcció....182
15.1 Introducció....183
15.2 Abast....184
15.3 Procediment de revisió per la direcció....185
15.3.1 Participants de la revisió....185
15.3.2 Agenda de la revisió....186
15.3.3 Periodicitat....187
16. Annex V: Gestió de Rols i Responsabilitats....188
16.1 Introducció....189
16.2 Abast....190
16.3 Organització de la seguretat de la informació....191
16.3.1 Comitè de seguretat de la informació....192
16.4 Rols i responsabilitats....194
16.4.1 Cap de seguretat o *Chief information security officer* (CISO)....194
16.4.2 Cap del departament de les tecnologies d'informació o *IT Manager*....194
16.4.3 El proveïdor de servei o *Service provider*....195
16.4.4 Director del centre de l'Organització....195
16.4.5 Treballadors....196
17. Annex VI: Metodologia d'Anàlisi de Riscos....197
17.1 Introducció....198
17.2 Abast....199
17.3 Metodologia d'anàlisi de riscos de l'Organització....200
17.3.1 Metodologia escollida: Magerit....200
17.3.2 Fase prèvia: Definició d'abast i establiment de paràmetres....200
17.3.3 Fase 1: Inventari i valoració d'actius....201
17.3.4 Fase 2: Anàlisi d'amenaces, impactes i vulnerabilitats....203
17.3.5 Fase 3: Determinació de l'impacte potencial....205
17.3.6 Fase 4: Nivell de risc acceptable i risc residual....205
18. Annex VII: Declaració d'Aplicabilitat....207
18.1 Introducció....208
18.2 Abast....209
18.3 Declaració d'aplicabilitat....210
19. Annex VIII: Informe d'auditoria de maig de 2022....225
19.1 Introducció....226
19.2 Abast....227
19.3 Normativa de referència....228
19.4 Informe d'auditoria....229
19.4.1 Data....229

19.4.2 Responsable....229
19.4.3 Nom de l’auditor o auditors....229
19.4.4 Abast....229
19.4.5 Controls auditats....229
19.4.6 Conformitat de l’SGSI amb els requisits de seguretat de l’Organització....252
19.4.7 Conformitat de l’SGSI amb la norma ISO/IEC 27001....254
19.4.8 No-conformitats detectades....264
19.4.9 Recomanacions de millora....268

Llista de figures

Figura 1: Diagrama Gantt de planificació del treball.....15
Figura 2: Organigrama general de l'Organització.....19
Figura 3: Anàlisi GAP dels requisits de la norma ISO/IEC 27001.....27
Figura 4: Anàlisi GAP dels controls definits a ISO/IEC 27002.....34
Figura 5: Arbre de dependències entre actius de l'Organització.....40
Figura 6: Evolució de l'anàlisi GAP dels requisits de la norma ISO/IEC 27001.....125
Figura 7: Evolució de l'anàlisi GAP dels controls definits a ISO/IEC 27002.....132
Figura 8: Organització de la seguretat de la informació.....191

Llista de taules

Taula 1: Nivells de maduresa del CMM aplicats a la seguretat de la informació.....21
Taula 2: CMM sobre els requisits de la ISO/IEC 27001.....25
Taula 3: CMM sobre els controls definits a ISO/IEC 27002.....33
Taula 4: Inventari dels actius de l'Organització.....39
Taula 5: Valoració dels actius de l'Organització.....43
Taula 6: Amenaces - actius de Personal.....44
Taula 7: Amenaces - actius d'Instal·lacions.....45
Taula 8: Amenaces - actius de Xarxa.....46
Taula 9: Amenaces - actius d'Equipament auxiliar (robots de cintes).....47
Taula 10: Amenaces - actius d'Equipament auxiliar (climatització i alimentació).....48
Taula 11: Amenaces - actius d'Equipament auxiliar (mobiliari).....48
Taula 12: Amenaces - actius de Hardware (routers, switches i tallafocs).....49
Taula 13: Amenaces - actius de Hardware (servidors).....50
Taula 14: Amenaces - actius de Hardware (laptops).....51
Taula 15: Amenaces - actius d'Aplicacions.....52
Taula 16: Amenaces - actius de Serveis.....52
Taula 17: Amenaces - actius de Dades.....53
Taula 18: Impacte potencial - amenaça: Incendi.....56
Taula 19: Impacte potencial - amenaça: Inundacions.....58
Taula 20: Impacte potencial - amenaça: Averia de l'equipament o programa (físic o lògic).....60
Taula 21: Impacte potencial - amenaça: Tall del subministre elèctric.....62
Taula 22: Impacte potencial - amenaça: Averia en el sistema de climatització.....64
Taula 23: Impacte potencial - amenaça: Incident en la xarxa de comunicacions.....66
Taula 24: Impacte potencial - amenaça: Error d'ús dels sistemes.....68
Taula 25: Impacte potencial - amenaça: Error d'administració dels sistemes.....69
Taula 26: Impacte potencial - amenaça: Incidents deguts a software malintencionat.....71
Taula 27: Impacte potencial - amenaça: Alteració de la informació.....73
Taula 28: Impacte potencial - amenaça: Destrucció de la informació.....75
Taula 29: Impacte potencial - amenaça: Fuga d'informació.....77
Taula 30: Impacte potencial - amenaça: Error de manteniment / actualització de software.....79
Taula 31: Impacte potencial - amenaça: Error de manteniment / actualització de hardware.....81
Taula 32: Impacte potencial - amenaça: Accés no autoritzat.....83
Taula 33: Impacte potencial - amenaça: Intercepció d'informació.....85
Taula 34: Risc de les amenaces.....86
Taula 35: Cost estimat - projecte 1: fase inicial.....89
Taula 36: Cost estimat - projecte 1: preparació de material.....90
Taula 37: Cost estimat - projecte 1: execució de campanyes.....91
Taula 38: Cost estimat - projecte 2: definició de tasques i recursos.....95
Taula 39: Cost estimat - projecte 2: implementació dels indicadors.....96
Taula 40: Cost estimat - projecte 2: gestió dels indicadors.....97
Taula 41: Cost estimat - projecte 3: definició de tasques i recursos.....100
Taula 42: Cost estimat - projecte 3: revisions per la direcció.....101
Taula 43: Cost estimat - projecte 3: auditories internes.....102
Taula 44: Cost estimat - projecte 3: auditories externes.....103
Taula 45: Cost estimat - projecte 4: definició de tasques i recursos.....108
Taula 46: Cost estimat - projecte 4: implantació de mesures.....109

Taula 47: Evolució del risc de les amenaces després dels projectes.....120
Taula 48: Evolució del CMM sobre els requisits de la ISO/IEC 27001 després dels projectes.....125
Taula 49: Evolució del CMM sobre els controls definits a ISO/IEC 27002 després dels projectes 132
Taula 50: Indicador - control de polítiques de seguretat.....167
Taula 51: Indicador - validesa de l'organització interna.....168
Taula 52: Indicador - control d'antecedents.....168
Taula 53: Indicador - mesura de la definició de les condicions i responsabilitats.....169
Taula 54: Indicador - mesura de campanyes de conscienciació.....169
Taula 55: Indicador - control de l'inventari d'actius.....170
Taula 56: Indicador - mesura del tipus d'informació.....170
Taula 57: Indicador - control de l'accés a xarxes, servidors i serveis.....171
Taula 58: Indicador - control de privilegis d'accés en cas de cessament d'activitats.....171
Taula 59: Indicador - control de privilegis d'accés en cas d'incorporació d'activitats.....172
Taula 60: Indicador - control d'inici de sessió segur.....172
Taula 61: Indicador - revisió de privilegis d'accés.....173
Taula 62: Indicador - control de l'accés físic a les instal·lacions de l'Organització.....173
Taula 63: Indicador - mesura de la seguretat a les instal·lacions i equips.....174
Taula 64: Indicador - control del manteniment dels equips i sistemes d'informació.....174
Taula 65: Indicador - control d'equip d'usuari desatès.....175
Taula 66: Indicador - mesura de la documentació de procediments d'operació.....175
Taula 67: Indicador - control del desplegament de software.....176
Taula 68: Indicador - control d'incidents de seguretat.....176
Taula 69: Indicador - control de backups i redundàncies.....177
Taula 70: Indicador - control de la gestió de la informació del registre d'events.....177
Taula 71: Indicador - control dels requeriments de xarxa i desenvolupament segurs.....178
Taula 72: Indicador - control de proves.....178
Taula 73: Indicador - control de documentació de relació amb proveïdors.....179
Taula 74: Indicador - control de procediments de gestió d'incidents de seguretat.....179
Taula 75: Indicador - control de la continuïtat del negoci.....180
Taula 76: Indicador - compliment de la legislació aplicable.....180
Taula 77: Indicador - revisió de la seguretat de la informació.....181
Taula 78: Valoració de les dimensions de seguretat.....202
Taula 79: Valoració dels actius.....203
Taula 80: Vulnerabilitat o probabilitat d'ocurrència.....204
Taula 81: Amenaces sobre un actiu.....205
Taula 82: Aplicabilitat dels controls ISO/IEC 27002 a l'Organització.....224
Taula 83: Auditoria sobre els controls ISO/IEC 27002 a l'Organització.....252
Taula 84: Auditoria sobre els objectius de seguretat de l'Organització.....254
Taula 85: Auditoria sobre els requisits de la norma ISO/IEC 27001 a l'Organització.....264

1. Introducció

1.1 Context i justificació del Treball

Les tecnologies de la informació tenen un paper cada cop més rellevant dins de la societat. Les activitats que es duen a terme en tots els àmbits, tant de caire empresarial com en un context més personal, augmenten contínuament la seva dependència en els sistemes d'informació. Aquesta dependència creixent, sumada al desenvolupament constant de noves amenaces, incrementa la importància que s'ha d'atorgar a aquests sistemes i a la seguretat de tots els aspectes que hi estan relacionats, en tant en quan la seguretat dels propis individus i les organitzacions en depèn directament.

El present treball es centra en analitzar quina és la importància dels aspectes de seguretat de la informació en l'àmbit d'una empresa determinada – que anomenarem Organització – i, més concretament, en el context dels seus processos de negoci més rellevants. Amb la realització d'aquest projecte voldrem determinar quina és la situació actual de l'Organització des del punt de vista de la seguretat, en base a estàndards i metodologies reconegudes internacionalment.

Tal i com es desprèn dels diferents capítols del treball, la seguretat de la informació és un aspecte prioritari dins de l'Organització, ja abans de l'elaboració del present projecte. L'anàlisi i redacció del mateix ens ajuda, però, a identificar quins són els aspectes i mesures que cal abordar per millorar el garantiment de les dimensions clàssiques de la seguretat per a l'Organització (confidencialitat, integritat, disponibilitat). Aquestes millores en matèria de seguretat repercutiran, a més, en el garantiment del compliment dels objectius de negoci de l'Organització.

1.2 Objectius del Treball

La realització del present treball persegueix els següents objectius:

- Determinar quin és l'estat actual de l'Organització en matèria de seguretat de la informació, de forma prèvia a la realització del projecte.
- Realitzar els diferents anàlisis i avaluacions en base a estàndards i metodologies reconegudes internacionalment (com ISO/IEC 27001 [3], ISO/IEC 27002 [1] o Magerit [12] [13] [14]), de manera que els resultats obtinguts siguin objectius i comparables a l'estat d'altres organitzacions.
- Identificar aspectes que cal millorar per a assolir i mantenir un nivell de seguretat adequat.

- Definir mesures tècniques i organitzatives per a tractar els aspectes a millorar.
- Assentar les bases per a la implantació d'un pla de seguretat a l'Organització, dissenyat en base a estàndards internacionals i encarat a un cicle de millora continua.
- Millorar el nivell de consciència sobre aspectes de seguretat de la informació.

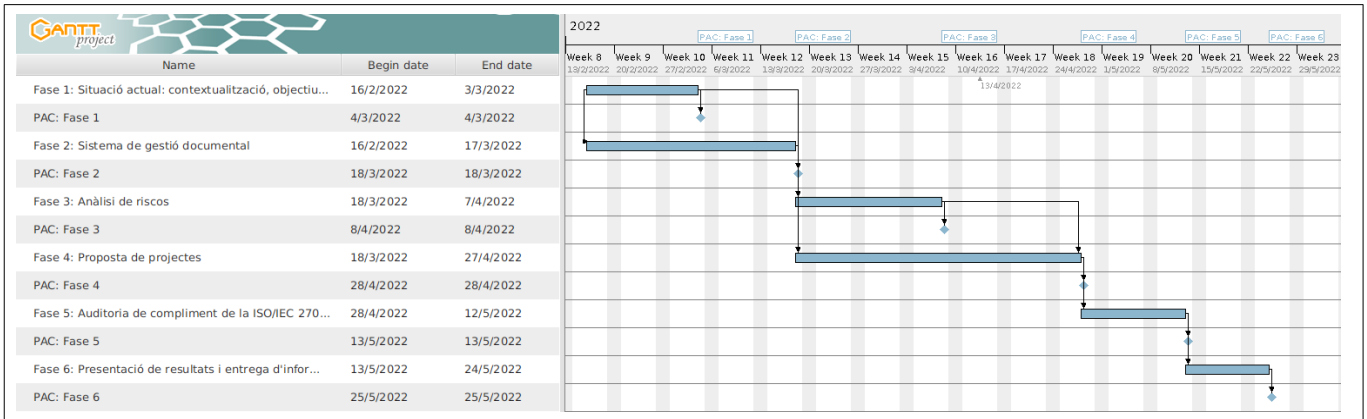
1.3 Enfocament i mètode seguit

La metodologia o aproximació escollida per a l'elaboració del present treball de màster és la realització de diferents fases – veure 1.4 per al desglossament de les fases –, mitjançant les quals es duu a terme un anàlisi exhaustiu de la situació actual de la seguretat de l'Organització i, a través de l'aplicació dels estàndards internacionals ISO/IEC 27001 [3] i ISO/IEC 27002 [1], es mira d'augmentar el nivell de seguretat existent. Un cop s'han aplicat les mesures de millora de l'SGSI de l'Organització – les propostes de projecte –, s'avalua quina ha estat l'evolució de la seguretat i, finalment, s'identifiquen elements on encara hi hauria potencial de creixement, en forma d'auditoria.

El mètode d'aproximació per fases al projecte afavoreix la consecució dels objectius del treball – veure 1.2 –, en tant en quan permet la focalització del treball en cadascun dels aspectes a tractar, cadascun dels quals serveix com a base indispensable per a la següent activitat.

1.4 Planificació del Treball

Les diferents tasques que cal dur a terme per a la realització del projecte s'agrupen en fases clarament definides, les quals coincideixen amb les fites parcials de cadascuna de les PAC a entregar. En la següent figura es mostren les fases en les que es descompon el present treball de màster, en forma de diagrama de Gantt, així com la planificació temporal i les relacions de dependència entre elles:



Name	Begin date	End date
Fase 1: Situació actual: contextualització, objectiu...	16/2/2022	3/3/2022
PAC: Fase 1	4/3/2022	4/3/2022
Fase 2: Sistema de gestió documental	16/2/2022	17/3/2022
PAC: Fase 2	18/3/2022	18/3/2022
Fase 3: Anàlisi de riscos	18/3/2022	7/4/2022
PAC: Fase 3	8/4/2022	8/4/2022
Fase 4: Proposta de projectes	18/3/2022	27/4/2022
PAC: Fase 4	28/4/2022	28/4/2022
Fase 5: Auditoria de compliment de la ISO/IEC 270...	28/4/2022	12/5/2022
PAC: Fase 5	13/5/2022	13/5/2022
Fase 6: Presentació de resultats i entrega d'infor...	13/5/2022	24/5/2022
PAC: Fase 6	25/5/2022	25/5/2022

Figura 1: Diagrama Gantt de planificació del treball

A continuació s'exposa una descripció breu de les fases mostrades a la figura 1:

- **Fase 1: Situació actual: contextualització, objectius i anàlisis diferencial**: En la primera fase del treball cal contextualitzar quina és la situació de partida, tant en forma de descripció de l'organització que es tractarà en el marc del treball i de l'abast de l'estudi, com en forma d'anàlisi de la situació actual de la seguretat. En quant al darrer punt, es duu a terme un anàlisi de compliment (o diferencial) respecte als requisits de la norma ISO/IEC 27001 [3] i a l'estat de maduresa dels controls ISO/IEC 27002 [1].

- **Fase 2: Sistema de gestió documental**: La segona fase del projecte consisteix en l'elaboració dels documents necessaris per a l'SGSI de l'Organització, segons defineix la norma ISO/IEC 27001. Aquesta fase es pot iniciar tan bon punt ha començat la fase de contextualització. La fase 2 és, a més, una de les que te més càrrega de treball associada de tot el projecte, degut a tota la documentació que cal generar.

- **Fase 3: Anàlisis de riscos**: En aquesta fase cal realitzar un anàlisi dels riscos intrínsecs als processos de negoci de l'Organització, en base a la metodologia Magerit. Per a iniciar la fase és necessari haver finalitzat les fases 1 i 2 (e.g. cal haver definit la metodologia). El resultat de la fase d'anàlisi de riscos és una visió objectiva i comparable, en tant que numèrica, de com afecten les diferents amenaces al tots els actius de l'Organització.

- **Fase 4: Proposta de projectes**: En la quarta fase del treball de màster es duen a terme propostes de projectes amb la finalitat de millorar l'estat actual de la seguretat de l'Organització. D'una banda, cal evolucionar l'estat de maduresa dels requisits de la norma ISO/IEC 27001 i dels controls de seguretat ISO/IEC 27002 i, d'altra banda, és necessari reduir el risc identificat a la fase anterior. Aquesta fase es pot iniciar tan

bon punt han finalitzat les fases 1 i 2. Per a concloure-la, a més, cal haver finalitzat l'anàlisi de riscos (fase 3).

- **Fase 5: Auditoria de compliment de la ISO/IEC 27002:2013**: En aquesta fase del projecte es duu a terme una auditoria de l'SGSI de l'Organització, les finalitats de la qual són, d'una banda, analitzar el compliment de la norma ISO/IEC 27001, dels controls ISO/IEC 27002 i dels objectius de seguretat definits i, d'altra banda, detectar i proposar oportunitats de millora. Totes aquestes avaluacions es realitzen suposant una implementació dels projectes proposats a la fase anterior, per la qual cosa cal haver finalitzat la fase 4 per a iniciar l'auditoria.

- **Fase 6: Presentació de resultats i entrega d'informes:** En l'última fase del treball cal finalitzar la memòria del projecte i realitzar el vídeo de defensa del mateix, el qual s'acompanya amb una presentació de suport. Es considera com a punt inicial de la darrera fase la finalització de totes les etapes anteriors.

1.5 Breu sumari de productes obtinguts

De la realització del present treball es desprèn, primerament, quina és la situació actual de l'Organització en relació a la seguretat de la informació – veure Anàlisi de compliment inicial i Anàlisi de riscos. Un cop s'ha analitzat detalladament l'estat de partida, es proposen mesures de millora – veure Proposta de projectes –, les quals possibilitarien una evolució del nivell de seguretat inicial. Les millores existents degut a l'aplicació dels projectes es troben recollides als capítols 7.6 , 7.7 i 7.8 . Finalment, i suposant una aplicació de tots els projectes proposats, es torna a realitzar un anàlisi de la situació existent; aquest cop, en forma d'auditoria, veure Auditoria de compliment de la ISO/IEC 27002:2013.

1.6 Breu descripció dels altres capítols de la memòria

A continuació es mostra una breu descripció dels capítols de la memòria i la seva relació amb el projecte global:

- Capítol 1. : Capítol introductori al present treball.
- Capítol 2. : Descripció de l'organització, a mode de context necessari per al desenvolupament dels següents apartats.
- Capítol 3. : Definició de l'abast del pla director de seguretat. Aquest abast és compartit per tots els documents, procediments i anàlisis efectuats.
- Capítol 4. : Avaluació de la situació actual de l'Organització, en base als requisits establerts a la norma ISO/IEC 27001 i als controls definits a ISO/IEC 27002.

- Capítol 5. : Introducció a la documentació requerida per la norma ISO/IEC 27001. Els documents es troben enllaçats en els annexos de la memòria.
- Capítol 6. : Anàlisi de riscos sobre els actius implicats en els processos de negoci de l'Organització.
- Capítol 7. : Proposta de projectes per a millorar els aspectes detectats en els anteriors apartats.
- Capítol 8. : Realització d'una auditoria de compliment, suposant una implementació dels projectes proposats.
- Capítol 9. : Conclusions extretes de la realització del present treball.
- Capítol 10. : Glossari de les abreviacions utilitzades durant la redacció del treball.
- Capítol 11. : Referències bibliogràfiques dels recursos utilitzats durant la redacció del treball.
- Annexos 12. a 19. : Informació complementària de naturalesa diversa: polítiques, reglaments, procediments, metodologies, la declaració d'aplicabilitat i l'informe d'auditoria detallat.

2. Descripció de l'Organització

L'organització analitzada com a subjecte del present treball de màster és una empresa dedicada principalment a la recerca en diverses disciplines. Per motius de confidencialitat, ens referirem a la mateixa durant tot el treball com a Organització.

L'esmentada organització està composta internament per multitud de centres o àrees de negoci, cadascun d'ells dedicats a la recerca en un o més àmbits. El centre que s'analitzarà te com a objectiu principal la realització d'estudis espai-temporals sobre diversos fenòmens naturals. Per a poder realitzar aquests estudis és necessari mantenir i tractar un gran volum de dades (tant en l'eix espacial com en el temporal), les quals es van processant amb una metodologia o una altra, en funció de la finalitat última de l'estudi que tractem. Aquestes dades, abans de poder ser tractades, també han de ser adquirides o generades, amb la qual cosa s'hauran de valorar els processos d'adquisició de les mateixes. Durant les diferents fases que conformen cadascun dels estudis, totes les dades s'han d'emmagatzemar de forma segura, considerant principalment les dimensions clàssiques de la seguretat de la informació: confidencialitat, integritat i disponibilitat. A mode d'exemple, es pot destacar que sovint les dades s'han d'emmagatzemar un mínim de 30 anys, per contracte. Un cop els estudis han assolit l'objectiu amb el qual van ésser dissenyats, sovint cal proporcionar aquests resultats a la comunitat científica. Aquest últim punt implica que serà necessari avaluar els processos de publicació de dades o resultats.

- El centre analitzat està compost per aproximadament 200 treballadors.
- Com acostuma a passar amb els centres de recerca, a l'Organització hi treballen empleats de diverses nacionalitats.
- Existeixen contractes nacionals i internacionals amb altres organitzacions, ja sigui per a l'adquisició de dades, per a la publicació de resultats, o per a la facilitació de serveis necessaris per a dur a terme els diferents processos de negoci. D'aquest punt s'extreu que hi ha contractes tant amb proveïdors com amb clients.
- Les dades estan emmagatzemades tant de forma localitzada com deslocalitzada.
- El processament i tractat de dades es realitza tant de forma local com de forma remota.
- L'organització disposa de seu física i de diversos equipaments informàtics i de comunicacions per a donar suport als processos de negoci.
- Les tasques realitzades per a complir amb els processos de l'Organització es duen a terme tant per part de treballadors interns com per subcontractistes.

En quant als diferents rols existents dins de l'organització, i les funcions i responsabilitats que cadascun d'aquests te associades, es pot trobar una definició dels mateixos, centrada en aspectes de seguretat de la informació, a Annex V: Gestió de Rols i Responsabilitats. En el mateix document també està documentada la organització de la seguretat de la informació. A continuació es mostra l'organigrama de l'Organització a un nivell general – no només

centrat en seguretat de la informació –, a fi i efecte de proporcionar una visió general sobre l'estructura interna de l'Organització. És necessari destacar que la definició es cenyeix al centre analitzat, no contemplant així la resta de centres de l'Organització.

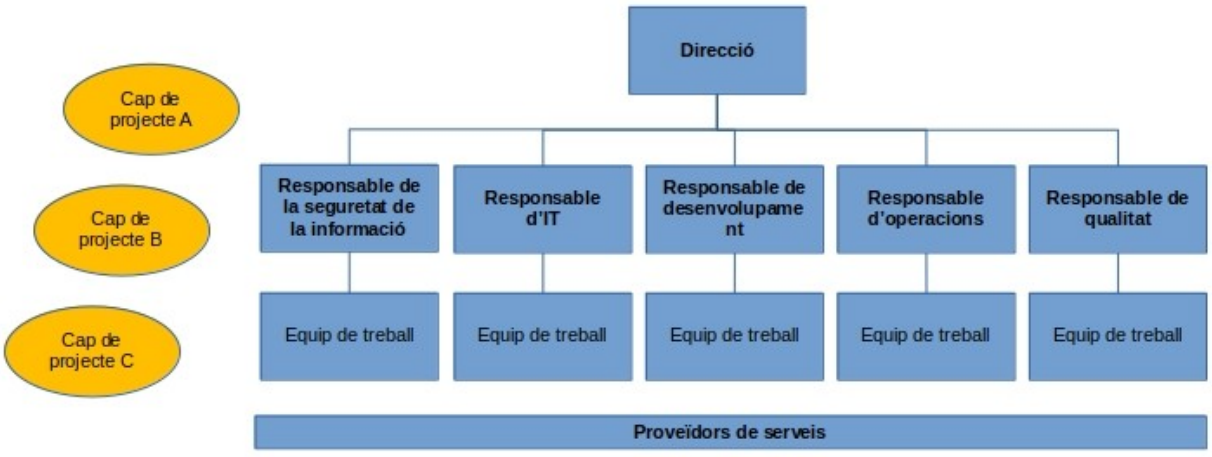


Figura 2: Organigrama general de l'Organització

Com es desprèn de l'organigrama proporcionat, la estructura interna de l'Organització està dividida diferents àrees de coneixement i una direcció conjunta de l'entitat. Per a cadascun dels equips de cada àrea, hi ha definit un responsable i un conjunt de treballadors. Per a realitzar les activitats de cadascuna de les àrees, l'Organització es recolza en la contractació de serveis per part de proveïdors, ja siguin aquests consultors especialitzats en temes concrets, o bé proveïdors de serveis base (e.g. servei de neteja, servei de comunicacions elèctriques, servei de xarxes, servei de cuina, etc).

Un aspecte destacable de l'Organització és la horitzontalitat en la gestió de projectes. En funció de la temàtica i característiques de cada projecte, i de les habilitats personals de cada treballador, la direcció assigna un cap de projecte dins d'una de les àrees de l'Organització, no havent de ser necessàriament aquest un dels responsables d'àrea. Es dona el cas, per tant, que dins d'alguns projectes un o més responsables d'àrea han de reportar a un empleat d'un equip de treball, al qual la direcció – en consens amb el responsable d'equip – li ha assignat el rol de cap de projecte. Al mateix torn aquest empleat pot estar treballant en altres projectes, liderats aquest cop per altres empleats de l'Organització.

3. Abast del pla director de seguretat

L'abast al qual es limita l'estudi i redacció del present treball de màster ja ha estat acotat anteriorment: de tots els àmbits de recerca que es duen a terme en el si de l'Organització, centrarem l'anàlisi sobre el centre que realitza estudis espai-temporals sobre diversos fenòmens naturals. Dins dels processos de negoci que suporten aquesta recerca, basarem l'anàlisi en les següents categories:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

Amb la finalitat de poder dur a terme els processos de les categories esmentades, també serà necessari analitzar altres aspectes de l'Organització, com: els actius físics i lògics implicats, els empleats, els proveïdors, els clients i la regulació aplicable.

4. Anàlisi de compliment inicial

L'anàlisi de compliment inicial de la norma ISO/IEC 27001 [3] per part de l'Organització és duu a terme mitjançant un anàlisi diferencial (o Anàlisi GAP) i fent ús del Model de Maduresa de la Capacitat (CMM, per les seves sigles en anglès *Capability Maturity Model*). Aquest model CMM conté 5 nivells, a més del nivell 0 o absència total, i el podem aplicar a la seguretat de la informació tal i com es mostra en la següent taula:

Nivell de maduresa	Significat
Nivell 0: INEXISTENT	No hi ha cap consciència ni definició respecte a la seguretat de la informació.
Nivell 1: INICIAL	Es duen a terme processos i procediments per part de les persones de la organització. Tot i així, això es fa de forma individual i sense basar-se en documentació existent.
Nivell 2: REPRODUÏBLE, PERÒ INTUÏTIU	Els processos i procediments per a assolir el mateix objectiu es duen a terme de manera similar, per part de diferents persones. Tot i així, això es fa en base a l'experiència adquirida, i no hi ha documentació formal al respecte. A més, sovint aquestes tasques es realitzen com a part d'altres activitats que no tenen a veure amb la seguretat de la informació.
Nivell 3: DEFINIT	Els processos i procediments, així com les responsabilitats en matèria de seguretat de la informació, han estat definits formalment i aquesta documentació s'ha donat a conèixer a tota la organització.
Nivell 4: GESTIONAT I MESURABLE	Els processos i procediments, a més d'estar definits i ser coneguts per tothom, poder ser mesurats i avaluats de forma qualitativa i quantitativa.
Nivell 5: OPTIMITZAT	Hi ha una avaluació i revisió contínua dels processos, procediments i les responsabilitats en matèria de seguretat de la informació, de manera que aquests es troben en un cicle de millora contínua.

Taula 1: Nivells de maduresa del CMM aplicats a la seguretat de la informació

D'una banda, apliquem aquest anàlisi als requisits de la norma ISO/IEC 27001 [3] i, d'altra banda, analitzem els controls definits a l'annex A de la norma o, altrament dit, als controls definits a la ISO/IEC 27002 [1].

4.1 Anàlisi de compliment inicial de la norma ISO/IEC 27001

En la següent taula es mostra l'anàlisi de compliment inicial de l'Organització en quant als requisits definits en la norma ISO/IEC 27001 [3].

Requisits	Nivell de maduresa actual
4: L'Organització i el Context	**2.16**
4.1: Entenent l'organització i el seu context	2.33
4.1.1: Estan identificats els objectius del SGS Sistema de Gestió de la Seguretat de la Informació?	3
4.1.2: S'han identificat les qüestions internes i externes relacionades amb la seguretat de la informació?	2
4.1.3: S'han identificat com les parts internes i externes poden suposar amenaces o riscos per a la seguretat de la informació?	2
4.2: Expectatives de les parts interessades	2.33
4.2.1: S'han identificat les parts interessades?	2
4.2.2: Hi ha un llistat de requisits sobre Seguretat de la Informació de les parts interessades?	2
4.2.3: Hi ha un llistat de requisits sobre Seguretat de la Informació referent a reglaments, requisits legals i requisits contractuals?	3
4.3: Abast del SGSI	2.00
4.3.1: S'ha determinat l'abast del SGS i se'n conserva informació documentada?	2
4.4: Sistema de Gestió de la Seguretat de la informació	2.00
4.4.1: El sistema de Gestió de Seguretat de la informació SGSI està establert, implementat i es revisa de manera planificada considerant oportunitats de millora?	2
5: Lideratge	**2.08**
5.1: Lideratge i compromís	2.00
5.1.1: S'han establert objectius de la Seguretat de la Informació d'acord amb els objectius del negoci?	3
5.1.2: La direcció proveeix dels recursos materials i humans necessaris per al compliment dels objectius del SGSI?	2
5.1.3: La direcció revisa directament l'eficàcia de l'SGSI per garantir que es compleixen els objectius de l'SGSI?	1
5.2: Política de la Seguretat de la Informació	2.25
5.2.1: S'ha definit una política de seguretat de la informació?	3
5.2.2: S'ha establert un marc que permeti establir objectius?	2
5.2.3: S'ha comunicat la política de seguretat de la informació a les parts interessades i a tota l'empresa?	1
5.2.4: Es manté informació documentada de la política de l'SGSI i dels seus objectius?	3
5.3: Rols i Responsabilitats	2.00

Requisits	Nivell de maduresa actual
5.3.1: S'han assignat les responsabilitats i les autoritats sobre la Seguretat de la Informació?	3
5.3.2: S'han comunicat convenientment les responsabilitats i les autoritats per a la Seguretat de la Informació?	1
6: Planificació	**2.07**
6.1: Tractament de Riscos i Oportunitats	1.80
6.1.1: El pla per abordar riscos i oportunitats considera les expectatives de les parts interessades en relació amb la seguretat de la informació?	2
6.1.2: S'identifiquen i analitzen els riscos mitjançant un mètode d'avaluació i d'acceptació de riscos?	2
6.1.3: S'ha definit un procés de tractament de riscos?	2
6.1.4: S'han establert criteris per elaborar una declaració d'aplicabilitat?	0
6.1.5: Es manté informació documentada dels punts anteriors?	3
6.2: Planificació per aconseguir objectius	2.33
6.2.1: S'han establert objectius de la Seguretat de la Informació mesurables i d'acord amb els objectius del negoci?	2
6.2.2: Els objectius de la Seguretat de la Informació estan planificats mitjançant? - Assignació de responsabilitats - Cronograma d'execució temporal - Mètode d'avaluació	2
6.2.3: S'han integrat els objectius de la Seguretat de la Informació als processos de l'organització tenint en compte les funcions principals dins de l'Organització?	3
7: Suport	**1.73**
7.1: Recursos	2.00
7.1.1: S'identifiquen i assignen els recursos necessaris per a l'SGSI?	2
7.2: Competència	1.50
7.2.1: S'avalua la competència en matèries de seguretat de la informació per a persones que efectuen tasques que puguin afectar la seguretat?	2
7.2.2: Es manté informació actualitzada sobre la competència del personal?	1
7.3: Conscienciació	2.50
7.3.1: El personal està involucrat i és conscient del seu paper a la Seguretat de la Informació?	2
7.3.2: Hi ha consciència dels danys que es poden produir de no seguir les pautes de la Seguretat de la Informació?	3
7.4: Comunicació	1.00
7.4.1: Es comunica la política de la Seguretat de la Informació amb les responsabilitats	1

Requisits	Nivell de maduresa actual
de cadascú?	
7.4.2: Hi ha un procés per comunicar les deficiències o males pràctiques en la seguretat de la informació?	1
7.5: Informació Documentada	1.67
7.5.1: Es disposa de la documentació requerida per la norma més la requerida per l'organització incloent-hi? - La política de la seguretat de la informació i l'abast del sistema de gestió - Els processos principals de la seguretat de la informació - Els documents exigits per la Norma ISO 27001 incloent registres - Els documents propis de seguretat de la informació identificats per l'empresa (instruccions tècniques etc.)	1
7.5.2: Hi ha un control documental on es verifica? - Qui publica el document - Qui ho autoritza i com es revisen - Formats i Suports de publicació - El seu emmagatzematge i protecció	2
7.5.3: Es controlen els documents d'origen extern?	2
8: Operació	**1.69**
8.1: Control Operacional	1.75
8.1.1: Els processos de seguretat de la informació estan documentats per controlar que es realitzen segons el planificat?	2
8.1.2: Hi ha un procés per avaluar els riscos a la Seguretat de la Informació abans de realitzar canvis en el Sistema de Gestió o processos de Seguretat?	2
8.1.3: S'estableixen mesures i plans per mitigar els riscos a la Seguretat de la Informació davant de canvis realitzats?	2
8.1.4: S'identifiquen i es controlen els processos externalitzats quant als riscos per a la Seguretat de la Informació?	1
8.2: Anàlisi de riscos de la Seguretat de la Informació	2.00
8.2.1: S'ha establert un procés documentat d'anàlisi i d'avaluació de riscos per a la seguretat de la informació on s'identifiqui? - El propietari del risc - La importància del risc o nivell d'impacte - La probabilitat d'ocurrència	2
8.3: Tractament de riscos de la Seguretat de la Informació	1.33
8.3.1: S'ha implementat un pla de tractament de risc on? - Els propietaris del risc estan informats i han aprovat el pla - Es documenten els resultats	2
8.3.2: S'identifiquen tots els controls necessaris per mitigar el risc justificant-ne l'aplicació?	1

Requisits	Nivell de maduresa actual
8.3.3: Es documenta el nivell d'aplicació de tots els controls que cal aplicar?	1
9: Avaluació de l'exercici	**1.05**
9.1: Seguiment i mesurament	0.50
9.1.1: S'ha establert un procés continu de monitorització dels aspectes clau de la seguretat de la informació tenint en compte els controls per a la seguretat de la informació?	1
9.1.2: S'ha establert un procés documentat per avaluar els resultats dels mesuraments i que aquests resultats són presos en compte pels responsables tant dels processos com de la Seguretat de la informació?	0
9.2: Auditories Internes	1.67
9.2.1: S'ha establert una programació d'auditories internes i assignat responsables?	2
9.2.2: L'abast i els requisits s'han definit per a l'informe d'auditoria?	1
9.2.3: Es consideren accions correctives i propostes de canvi als informes d'auditoria?	2
9.3: Informe de Revisió per la Direcció	1.00
9.3.1: Hi ha una programació per als informes de la direcció i hi ha constància de la seva realització periòdica?	1
9.3.2: Es documenten els resultats dels informes i la direcció s'implica tant en el coneixement com en la presa de decisions sobre els aspectes crucials per al SGSI?	1
10: Millora	**0.75**
10.1: No Conformitats i accions correctives	0.50
10.1.1: Hi ha un procediment documentat per identificar i registrar les no-conformitats i el seu tractament?	1
10.1.2: Dins de les accions correctives hi ha una diferenciació entre accions correctives sobre la no-conformitat i sobre les causes de la mateixa?	0
10.2: Millora continua	1.00
10.2.1: Hi ha un procés per garantir la millora contínua de l'SGSI identificant les oportunitats de millora?	1

Taula 2: CMM sobre els requisits de la ISO/IEC 27001

Com es desprèn de la taula 2, tant els objectius de l'SGSI de l'Organització com les qüestions de context, les parts interessades i els seus requisits en seguretat de la informació, es troben definides, tot i que no d'una manera objectivament mesurable. A més, manca sovint una comunicació d'aquests aspectes al conjunt de l'Organització. El fet de la comunicació és un aspecte millorable en molts àmbits de l'SGSI de l'Organització.

En quant al lideratge, podem afirmar que els objectius de l'SGSI estan definits amb la intervenció de la direcció i, d'aquesta manera, estan alineats amb les necessitats de negoci

de l’Organització. Existeix també una política de seguretat de la informació i una definició de rols i responsabilitats. Com a punt negatiu es pot destacar la manca de revisions periòdiques, a més de la falta de comunicació corporativa ja esmentada.

Existeix un anàlisi de riscos, accessible sota demanda, tot i que la seva existència no ha estat comunicada a totes les parts interessades de l’Organització. Manca completament una declaració d’aplicabilitat o els criteris per a establir-la.

En quant a l’apartat de suport de la norma ISO/IEC 27001, destaca negativament la periodicitat de les revisions i actualitzacions de la competència del personal, així com la manca de comunicació de documentació rellevant en seguretat de la informació dins de l’Organització, com e.g. la política de seguretat de la informació.

En les operacions dels diversos processos de l’Organització, tot i que existeixen procediments i processos per avaluar riscos, en alguns punts hi ha aspectes a millorar per a complir amb la norma ISO/IEC 27001, com pot ser en allò relacionat amb la documentació exhaustiva dels controls necessaris a implementar.

Degut a manca de controls clarament definits o, si més no, d’indicadors que permetin realitzar un seguiment i mesurament objectius, l’avaluació de l'exercici és un apartat que te un gran potencial de millora. El mateix passa amb les revisions, principalment per la falta de reavaluacions periòdiques. Sí que es duen a terme, en canvi, auditories internes per avaluar l’estat actual de l’SGSI, si bé no amb una periodicitat prefixada ni seguint un estàndard internacional.

Finalment, l’apartat de millora continua és un dels que parteix d’una situació inicial més negativa, en gran mesura degut a la manca de seguiment, mesurament i revisió esmentada en el punt anterior.

Els aspectes esmentats els podem observar també reflectits en el següent gràfic de maduresa general, en forma d’anàlisi GAP.

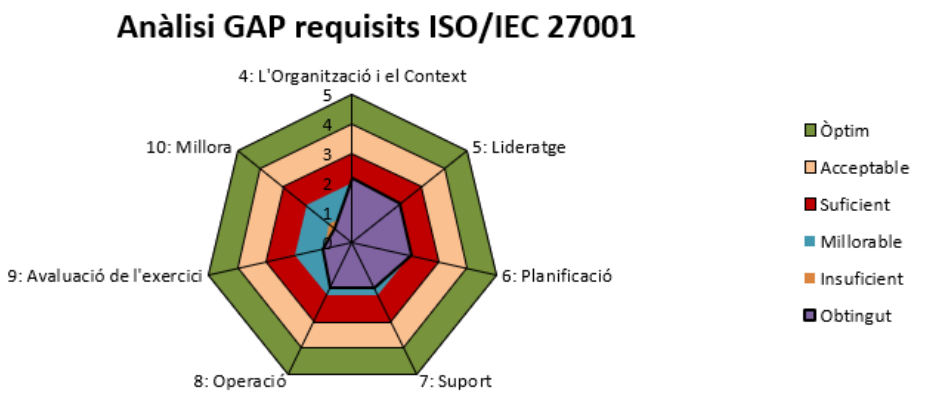


Figura 3: Anàlisi GAP dels requisits de la norma ISO/IEC 27001

4.2 Anàlisi de compliment inicial dels controls ISO/IEC 27002

En la següent taula es mostra l'anàlisi de compliment inicial de l'Organització en quant als controls definits en l'ISO/IEC 27002 [1].

Control	Nivell de maduresa actual
A.5: Polítiques de seguretat de la informació	**2.00**
A.5.1: Directrius de gestió de la seguretat de la informació	2.00
A.5.1.1: Polítiques per la seguretat de la informació	3
A.5.1.2: Revisió de les polítiques per la seguretat de la informació	1
A.6: Organització de la seguretat de la informació	**2.50**
A.6.1: Organització interna	2.00
A.6.1.1: Rols i responsabilitats en seguretat de la informació	3
A.6.1.2: Segregació de tasques	3
A.6.1.3: Contacte amb les autoritats	1
A.6.1.4: Contacte amb grups d'interès especial	2
A.6.1.5: Seguretat de la informació en la gestió de projectes	1
A.6.2: Els dispositius mòbils i el teletreball	3.00
A.6.2.1: Política de dispositius mòbils	3
A.6.2.2: Teletreball	3
A.7: Seguretat relativa als recursos humans	**2.56**

Control	Nivell de maduresa actual
A.7.1: Abans del treball	3.00
A.7.1.1: Investigació d’antecedents	3
A.7.1.2: Condicions de treball	3
A.7.2: Durant el treball	1.67
A.7.2.1: Responsabilitats de gestió	2
A.7.2.2: Conscienciació, educació i capacitació en seguretat de la informació	2
A.7.2.3: Procés disciplinari	1
A.7.3: Finalització del treball o canvi de lloc de treball	3.00
A.7.3.1: Responsabilitats davant la finalització o canvi	3
A.8: Gestió d’actius	**2.00**
A.8.1: Responsabilitat sobre els actius	2.00
A.8.1.1: Inventari d’actius	3
A.8.1.2: Propietat dels actius	1
A.8.1.3: Ús acceptable dels actius	2
A.8.1.4: Devolució d’actius	2
A.8.2: Classificació de la informació	2.33
A.8.2.1: Classificació de la informació	3
A.8.2.2: Etiquetat de la informació	2
A.8.2.3: Manipulació de la informació	2
A.8.3: Manipulació dels suports	1.67
A.8.3.1: Gestió de suports extraïbles	2
A.8.3.2: Eliminació de suports	2
A.8.3.3: Suports físics en trànsit	1
A.9: Control d’accés	**2.52**
A.9.1: Requisits de negoci pel control d’accés	2.00
A.9.1.1: Política de control d’accés	2
A.9.1.2: Accés a les xarxes i als servidors de xarxa	2
A.9.2: Gestió d’accés d’usuari	2.67
A.9.2.1: Registre i baixa d’usuari	3
A.9.2.2: Provisió d’accés d’usuari	3
A.9.2.3: Gestió de privilegis d’accés	2
A.9.2.4: Gestió de la informació secreta d’autenticació dels usuaris	2

Control	Nivell de maduresa actual
A.9.2.5: Revisió dels drets d’accés d’usuari	3
A.9.2.6: Retirada o reassignació dels drets d’accés	3
A.9.3: Responsabilitats de l’usuari	3.00
A.9.3.1: Ús de la informació secreta d’autenticació	3
A.9.4: Control d’accés a sistemes i aplicacions	2.40
A.9.4.1: Restricció de l’accés a la informació	2
A.9.4.2: Procediments d’inici de sessió	3
A.9.4.3: Sistema de gestió de contrasenyes	3
A.9.4.4: Ús d’utilitats amb privilegis del sistema	3
A.9.4.5: Control d’accés al codi font dels programes	1
A.10: Criptografia	**2.00**
A.10.1: Controls criptogràfics	2.00
A.10.1.1: Política d’usos dels controls criptogràfics	2
A.10.1.2: Gestió de claus	2
A.11: Seguretat física i de l’entorn	**1.83**
A.11.1: Àrees segures	1.67
A.11.1.1: Perímetre de seguretat física	3
A.11.1.2: Controls físics d’entrada	4
A.11.1.3: Seguretat d’oficines, despatxos i recursos	0
A.11.1.4: Protecció contra les amenaces externes i ambientals	3
A.11.1.5: El treball en àrees segures	0
A.11.1.6: Àrees de càrrega i descàrrega	0
A.11.2: Seguretat dels equips	2.00
A.11.2.1: Emplaçament i protecció d’equips	3
A.11.2.2: Instal·lacions de subministrament	3
A.11.2.3: Seguretat del cablejat	2
A.11.2.4: Manteniment dels equips	3
A.11.2.5: Retirada de materials propietat de la empresa	0
A.11.2.6: Seguretat dels equips fora de les instal·lacions	2
A.11.2.7: Reutilització o eliminació segura d’equips	2
A.11.2.8: Equip d’usuari desatès	2
A.11.2.9: Política de lloc de treball ordenat i pantalla neta	1

Control	Nivell de maduresa actual
A.12: Seguretat de les operacions	**1.96**
A.12.1: Procediments i responsabilitats operacionals	2.25
A.12.1.1: Documentació de procediments d'operació	2
A.12.1.2: Gestió de canvis	1
A.12.1.3: Gestió de capacitats	3
A.12.1.4: Separació dels recursos de desenvolupament, prova i operació	3
A.12.2: Protecció contra software maliciós (*malware*)	2.00
A.12.2.1: Controls contra el codi maliciós	2
A.12.3: Còpies de seguretat	3.00
A.12.3.1: Còpies de seguretat de la informació	3
A.12.4: Registres i supervisió	2.00
A.12.4.1: Registre d'events	2
A.12.4.2: Protecció de la informació del registre	1
A.12.4.3: Registres d'administració i operació	2
A.12.4.4: Sincronització del rellotge	3
A.12.5: Control del software en explotació	1.00
A.12.5.1: Instal·lació del software en explotació	1
A.12.6: Gestió de la vulnerabilitat tècnica	2.50
A.12.6.1: Gestió de les vulnerabilitats tècniques	2
A.12.6.2: Restricció en la instal·lació de software	3
A.12.7: Consideracions sobre l'auditoria de sistemes d'informació	1.00
A.12.7.1: Controls d'auditoria de sistemes d'informació	1
A.13: Seguretat de les comunicacions	**2.08**
A.13.1: Gestió de la seguretat de xarxes	2.67
A.13.1.1: Controls de xarxa	3
A.13.1.2: Seguretat dels serveis de xarxa	2
A.13.1.3: Segregació en xarxes	3
A.13.2: Intercanvi d'informació	1.50
A.13.2.1: Polítiques i procediments d'intercanvi d'informació	1
A.13.2.2: Acords d'intercanvi d'informació	2
A.13.2.3: Missatgeria electrònica	1
A.13.2.4: Acords de confidencialitat o no revelació	2

Control	Nivell de maduresa actual
A.14: Adquisició, desenvolupament i manteniment dels sistemes d’informació	**1.81**
A.14.1: Requisits de seguretat en els sistemes d’informació	1.67
A.14.1.1: Anàlisi de requisits i especificacions de seguretat de la informació	1

Control	Nivell de maduresa actual
A.14.1.2: Assegurar els serveis d'aplicacions en xarxes públiques	3
A.14.1.3: Protecció de les transaccions de serveis d'aplicacions	1
A.14.2: Seguretat en el desenvolupament i en els processos de suport	1.78
A.14.2.1: Política de desenvolupament segur	1
A.14.2.2: Procediment de control de canvis en sistemes	2
A.14.2.3: Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu	2
A.14.2.4: Restriccions als canvis als paquets de software	2
A.14.2.5: Principis d'enginyeria de sistemes segurs	2
A.14.2.6: Entorn de desenvolupament segur	2
A.14.2.7: Externalització del desenvolupament de software	2
A.14.2.8: Proves funcionals de seguretat de sistemes	1
A.14.2.9: Proves d'acceptació de sistemes	2
A.14.3: Dades de prova	2.00
A.14.3.1: Protecció de les dades de prova	2
A.15: Relació amb proveïdors	**2.00**
A.15.1: Seguretat en les relacions amb proveïdors	2.00
A.15.1.1: Política de seguretat de la informació en les relacions amb els proveïdors	3
A.15.1.2: Requisits de seguretat en contractes amb tercers	2
A.15.1.3: Cadena de subministrament de tecnologia de la informació i de les comunicacions	1
A.15.2: Gestió de la provisió de serveis del proveïdor	2.00
A.15.2.1: Control i revisió de la provisió de serveis del proveïdor	2
A.15.2.2: Gestió de canvis en la provisió del servei del proveïdor	2
A.16: Gestió d'incidents de seguretat de la informació	**1.86**
A.16.1: Gestió d'incidents de seguretat de la informació i millores	1.86
A.16.1.1: Responsabilitats i procediments	3
A.16.1.2: Notificació dels events de seguretat de la informació	2
A.16.1.3: Notificació de punts dèbils de la seguretat	1
A.16.1.4: Avaluació i decisió sobre els events de seguretat de la informació	2
A.16.1.5: Resposta a incidents de seguretat de la informació	2
A.16.1.6: Aprenentatge dels incidents de seguretat de la informació	2
A.16.1.7: Recopilació d'evidències	1

Control	Nivell de maduresa actual
A.17: Aspectes de seguretat de la informació per a la gestió de la continuïtat del negoci	**2.67**
A.17.1: Continuïtat de la seguretat de la informació	2.33
A.17.1.1: Planificació de la continuïtat de la seguretat de la informació	2
A.17.1.2: Implementar la continuïtat de la seguretat de la informació	3
A.17.1.3: Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació	2
A.17.2: Redundàncies	3.00
A.17.2.1: Disponibilitat dels recursos de tractament de la informació	3
A.18: Compliment	**1.83**
A.18.1: Compliment dels requisits legals i contractuals	2.00
A.18.1.1: Identificació de la legislació aplicable i dels requisits contractuals	2
A.18.1.2: Drets de propietat intel·lectual (DPI)	2
A.18.1.3: Protecció dels registres de la organització	1
A.18.1.4: Protecció i privacitat de la informació de caràcter personal	3
A.18.1.5: Regulació dels controls criptogràfics	2
A.18.2: Revisions de la seguretat de la informació	1.67
A.18.2.1: Revisió independent de la seguretat de la informació	1
A.18.2.2: Compliment de les polítiques i normes de seguretat	2
A.18.2.3: Comprovació del compliment tècnic	2

Taula 3: CMM sobre els controls definits a ISO/IEC 27002

En la taula 3 veiem una tendència general a no superar el valor 3 o DEFINIT. Això sol estar ocasionat per la manca de mesures clares i objectives de mesurament, que impedeixen trobar-se a un nivell 4 o GESTIONAT I MESURABLE, i que possibilitarien, al seu torn, l'oportunitat d'arribar a un nivell 5 o OPTIMITZAT, en el cas que s'establissin també mecanismes i procediments de revisió periòdica.

En quant a controls o categories de controls concrets que destaquen pel seu baix nivell d'implantació actual, podem destacar:

- Seguretat en la gestió de projectes i en l'anàlisi de requisits i enginyeria dels sistemes. A vegades no se li atorga la importància necessària als aspectes relacionats amb la seguretat de la informació. Exemples de controls: A.6.1.5, A.14.1.1, A.14.1.3 i A.14.2.1. En aquest cas, podem parlar de manca del concepte de *Security by Design.*

- Tractament i documentació dels actius i dels tipus d'informació de manera consistent, especialment quan es refereix a mantenir-ne propietats actualitzades, com e.g. el seu propietari.
- Alguns controls de la categoria d'àrees segures. Aquests, però, no apliquen en l'àmbit de les activitats de l'Organització, com es mostra a Annex VII: Declaració d'Aplicabilitat.
- Alguns procediments que, tot i existir, no estan definits de manera homogènia per a tots els processos similars dins de l'Organització, sinó que cada grup de treball actua de forma independent. Exemples en són el control A.12.1.2 i els controls en matèria d'intercanvi d'informació.
- Consideració d'aspectes de seguretat de la informació quan es realitzen proves i avaluacions per a acceptar el software a entorns productius. És habitual que l'anàlisi es centri en aspectes funcionals i rendiment, obviant els aspectes de seguretat. Exemples de controls: A.12.5.1, A.14.2.8 i A.14.2.9.
- Controls relacionats amb revisions i notificació d'informacions, com poden ser: A.16.1.2, A.16.1.3, A.17.1.3 i 18.2.1.

Els aspectes esmentats els podem observar també reflectits en el següent gràfic de maduresa general, en forma d'anàlisi GAP.

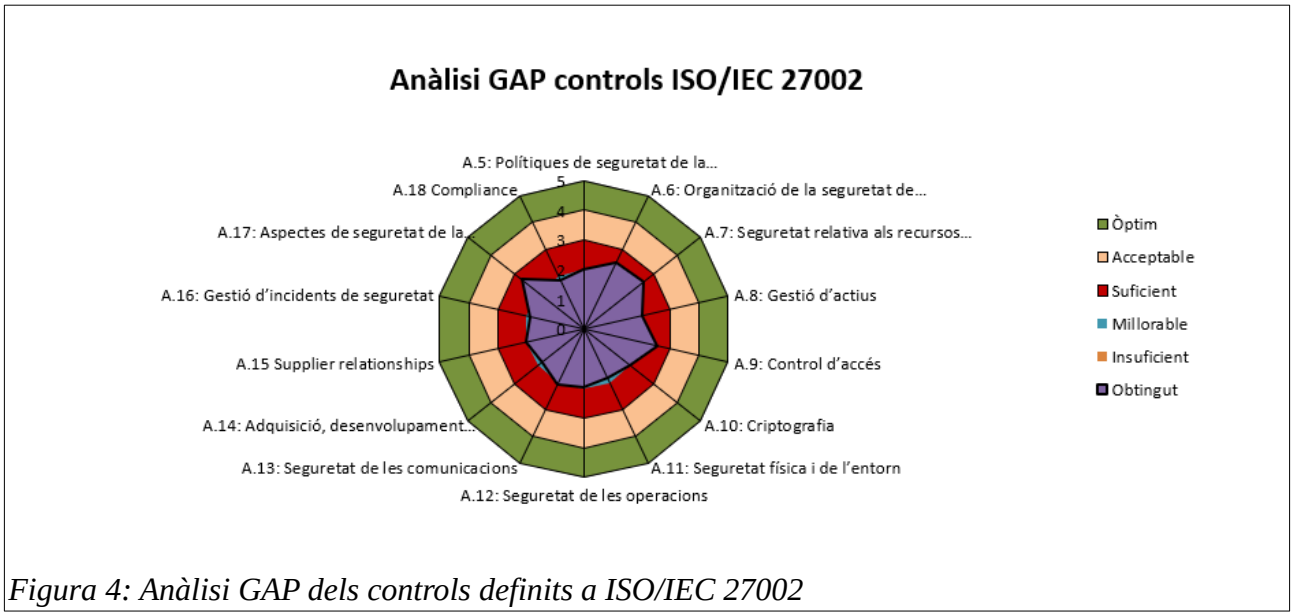


Figura 4: Anàlisi GAP dels controls definits a ISO/IEC 27002

5. Esquema documental ISO/IEC 27001

La norma ISO/IEC 27001 defineix un conjunt de documents necessaris per a la correcta definició i implementació d'un SGSI. En el cas del present pla director de seguretat de l'Organització, l'esquema documental està conformat pels següents documents:

- Política de Seguretat
- Procediment d'Auditories Internes
- Gestió d'Indicadors
- Procediment de Revisió per Direcció
- Gestió de Rols i Responsabilitats
- Metodologia d'Anàlisi de Riscos
- Declaració d'Aplicabilitat

5.1 Política de Seguretat

La política de seguretat de l'Organització és el document de més alt nivell que fa referència a la política global de l'SGSI, a més de definir-ne els seus objectius, el marc regulador aplicable, fer referència al conjunt de polítiques i reglaments de l'Organització, i descriure breument els rols i responsabilitats existents dins de l'Organització, en matèria de seguretat de la informació.

La política de seguretat es troba adjuntada a l'annex 12. .

5.2 Procediment d'Auditories Internes

A l'annex 13. defineix el procediment sobre com s'han d'organitzar, preparar i executar les auditories internes en l'àmbit de l'SGSI de l'Organització, les quals són un mecanisme molt efectiu per avaluar d'una forma objectiva l'estat de l'SGSI. A més, aquestes són un requisit indispensable per a ser conforme amb la clàusula 9.2 de la norma ISO/IEC 27001 [3].

5.3 Gestió d'Indicadors

Un cop s'han dissenyat i implementat els controls de seguretat de l'SGSI de l'Organització, i com a pas imprescindible per a poder mantenir aquest en un procés de constant revisió i

millora, cal definir indicadors, els quals possibiliten el monitoratge dels controls de seguretat. A l'annex 14. es troben descrits els indicadors de seguretat que es faran servir a l'Organització, així com el mètodes de seguiment, mesurament, anàlisi i avaluació utilitzats.

5.4 Procediment de Revisió per Direcció

Cal dur a terme revisions periòdiques de l'SGSI de l'Organització. Aquestes revisions, segons marca la clàusula 9.3 de la norma ISO/IEC 27001 [3], han de ser realitzades per part de la direcció de l'entitat, per ser aquesta la part de l'estructura organitzativa amb més potestat de decisió, també en matèria de seguretat de la informació. El procediment al respecte està documentat a l'annex 15. del present document.

5.5 Gestió de Rols i Responsabilitats

Es defineixen els diferents rols, amb funcions i responsabilitats associades, que existeixen en l'Organització, en matèria de seguretat de la informació. Aquesta documentació es pot trobar de forma adjunta, a l'annex 16. .

5.6 Metodologia d'Anàlisi de Riscos

Un dels eixos centrals de la definició i implementació de l'SGSI de l'Organització és la realització de l'anàlisi de riscos dels actius de la mateixa. Amb la finalitat de descriure els passos necessaris per a dur-lo a terme, es troba definit a l'annex 17. la metodologia que es fa servir per a la realització de l'esmentat anàlisi de risc.

5.7 Declaració d'Aplicabilitat

Un dels requisits de la norma ISO/IEC 27001 [3] és seleccionar i implantar els controls proposats a l'annex A de la mateixa [1]. Els controls definits en aquest annex també es coneixen com a ISO/IEC 27002. En el cas de l'SGSI de l'Organització, s'ha avaluat i decidit quins d'aquests controls apliquen als processos de negoci i quins no. Aquesta informació, anomenada formalment Declaració d'Aplicabilitat, es troba adjunta a l'annex 18. del present document.

6. Anàlisi de riscos

Una de les etapes principals del pla director de seguretat de l'Organització és la realització de l'anàlisi de riscos. En el present apartat es duu a terme dit anàlisi, seguint el procediment definit a l'annex 17. i que, al seu torn, està basat en la metodologia Magerit – veure els llibres Magerit [12], [13] i [14].

6.1 Abast

L'abast de l'anàlisi de riscos coincideix amb l'abast general definit al pla director de seguretat de l'Organització. És a dir, s'identificaran i avaluaran els riscos intrínsecs als actius que participen en la preparació i posada en pràctica dels següents processos de negoci:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

6.2 Inventari d'actius

Seguint el procediment establert a l'annex 17. , en la primera fase de l'anàlisi s'identifiquen els actius de l'Organització que estan vinculats als processos de negoci inclosos a l'abast de l'anàlisi. La següent taula conté el llistat dels actius rellevants i el seu propietari, a més de la categoria a la qual pertanyen, d'entre les definides al llibre I de la metodologia Magerit [12].

Àmbit	Actiu	Propietari
Instal·lacions	Edifici oficines i CPD	*IT Manager*
Instal·lacions	Edifici CPD de *backup*	*IT Manager*
Hardware	*Router* principal - primari	*IT Manager*
Hardware	*Router* principal - *backup*	*IT Manager*
Hardware	*Switches* oficines	*IT Manager*
Hardware	*Switches* sales de reunions	*IT Manager*

Àmbit	Actiu	Propietari
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)	CISO
Hardware	Tallafocs extern (entre la DMZ i Internet)	CISO
Hardware	Servidors d'adquisició (a la DMZ)	*IT Manager*
Hardware	Servidors de publicació (a la DMZ)	*IT Manager*
Hardware	Servidors d'emmagatzematge (al *backend*)	*IT Manager*
Hardware	Servidors de processament (al *backend*)	*IT Manager*
Hardware	*Laptops*	*IT Manager*
Aplicacions	Gestor de màquines virtuals	Responsable d'operacions
Aplicacions	Sistema operatiu dels servidors	Responsable d'operacions
Aplicacions	Software d'adquisició	Responsable d'operacions
Aplicacions	Software de publicació	Responsable d'operacions
Aplicacions	Software d'emmagatzematge	Responsable d'operacions
Aplicacions	Software de processament	Responsable d'operacions
Dades	Dades *input* dels estudis	Cap de projecte corresponent
Dades	Dades *output* dels estudis o resultats	Cap de projecte corresponent
Dades	Credencials d'accés als sistemes	CISO
Dades	Dades personals d'empleats	Direcció
Dades	Registres d'activitat	CISO
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)	Cap de projecte corresponent
Dades	Codi font del software propi	Responsable de desenvolupament
Xarxa	Xarxa administrativa	*IT Manager*
Xarxa	Xarxa interna transferència de dades	*IT Manager*
Xarxa	Connexió a Internet - primària	*IT Manager*
Xarxa	Connexió a Internet - *backup*	*IT Manager*
Serveis	Servei de directori	Responsable d'operacions
Serveis	Servei FTP	Responsable d'operacions
Serveis	Servei HTTP	Responsable d'operacions
Serveis	Servei de correu electrònic	Responsable d'operacions

Àmbit	Actiu	Propietari
Serveis	Servei d’accés remot o VPN	Responsable d’operacions
Equipament auxiliar	Robot de cintes d’emmagatzematge - primari	*IT Manager*
Equipament auxiliar	Robot de cintes d’emmagatzematge - *backup*	*IT Manager*
Equipament auxiliar	Climatització del CPD primari	*IT Manager*
Equipament auxiliar	Climatització del CPD de *backup*	*IT Manager*
Equipament auxiliar	Alimentació dels sistemes	*IT Manager*
Equipament auxiliar	Alimentació dels sistemes - *backup* o *UPS*	*IT Manager*
Equipament auxiliar	Mobiliari oficines	*IT Manager*
Equipament auxiliar	Mobiliari sales de reunions	*IT Manager*
Personal	Administradors de xarxes / subcontractistes	Direcció
Personal	Administradors de sistemes / subcontractistes	Direcció
Personal	Operadors	Direcció
Personal	Desenvolupadors	Direcció
Personal	Proveïdors de serveis	Direcció

Taula 4: Inventari dels actius de l’Organització

Els actius de l’Organització estan interrelacionats els uns amb els altres. A continuació es mostra l’arbre de dependències entre ells.

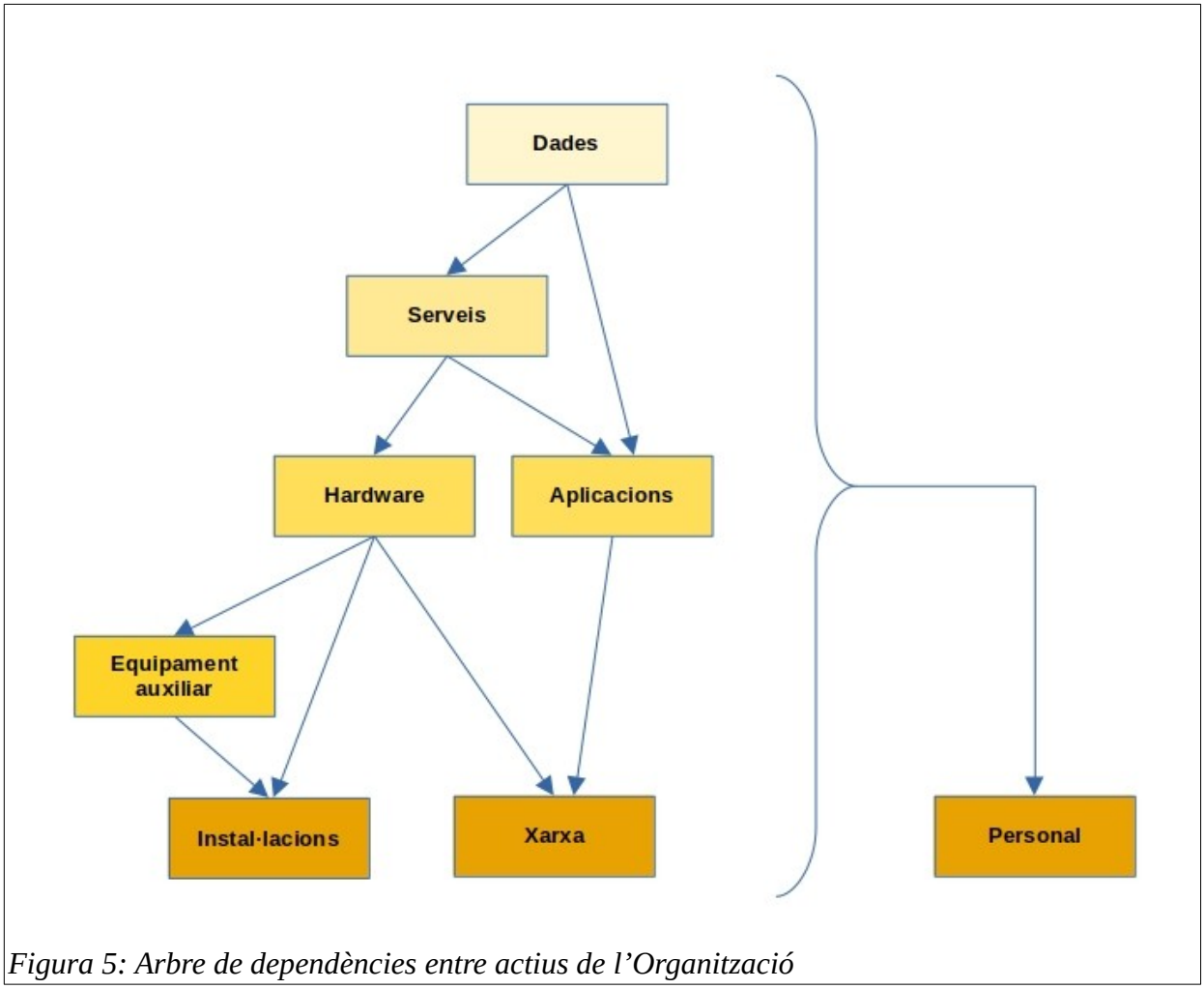


Figura 5: Arbre de dependències entre actius de l'Organització

Les dependències existents entre els actius venen definides en funció de la categoria a la qual pertanyen. La figura mostra, per tant, els actius de quina categoria poden dependre dels actius d'una altra. En l'àmbit de l'anàlisi de riscos, les dependències indiquen quins actius «superiors» es veuran afectats per una degradació en els actius «inferiors» en els quals els primers es sustenten.

Com es desprèn de la figura 5, els actius de les categories Instal·lacions i Xarxa són la base dels processos de negoci de l'Organització, sense els quals la resta d'actius no aporten valor a la mateixa. Els actius d'aquestes categories actuen com a actius «inferiors» dels de tipus Equipament auxiliar, Hardware i Aplicacions. Els actius de la categoria Equipament auxiliar, al seu torn, fan la funció d'actius «inferiors» respecte als de tipus Hardware. D'altra banda, els actius de la categoria Serveis actuen com a actius «superiors» de Hardware i d'Aplicacions i d'actius «inferiors» de la categoria de Dades. Aquesta última dependència és també compartida pels actius de la categoria d'Aplicacions. Finalment, els treballadors de l'Organització, els proveïdors de serveis i els subcontractistes (tots ells formant part de la

categoria Personal) actuen com a actius «inferiors» de tots els altres actius, ja que sense ells cap dels processos de negoci és possible.

Les dependències exposades no apliquen necessàriament a la totalitat dels actius de cada categoria: per exemple, una incidència en el mobiliari d'oficines (categoria Equipament auxiliar) no comporta una afectació als servidors de processament (categoria Hardware). En canvi, la mateixa incidència sí que afectarà als *laptops* dels treballadors que es trobin a l'oficina i als *switches* d'oficines (ambdós pertanyen també a la categoria Hardware). En passos posteriors de l'anàlisi de riscos – càlcul de l'impacte de les amenaces – es te en compte l'existència o no de la dependència.

6.3 Taula de valoracions

En quant a les valoracions dels actius, i segons es defineix a l'annex 17.3 , aquests cal avaluar-los segons el valor que tenen dins de l'Organització («Valor»), a més d'indicar-ne quin greuge causaria als processos de negoci una afectació de l'actiu en cadascuna de les dimensions ACID. La següent taula mostra aquesta valoració.

Àmbit	Actiu	Valor	Aspectes crítics				
			A	C	I	D	T
Instal·lacions	Edifici oficines i CPD	MA	4	5	5	10	7
Instal·lacions	Edifici CPD de *backup*	A	4	5	5	6	7
Hardware	*Router* principal - primari	MA	5	8	8	9	8
Hardware	*Router* principal - *backup*	M	5	8	8	6	8
Hardware	*Switches* oficines	M	4	6	4	3	3
Hardware	*Switches* sales de reunions	M	4	6	4	3	3
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)	A	8	4	6	8	8
Hardware	Tallafocs extern (entre la DMZ i Internet)	MA	8	4	6	10	8
Hardware	Servidors d'adquisició (a la DMZ)	A	6	3	6	7	5
Hardware	Servidors de publicació (a la DMZ)	MA	4	5	5	8	6
Hardware	Servidors d'emmagatzematge (al *backend*)	MA	6	7	10	8	3
Hardware	Servidors de processament (al *backend*)	A	3	4	7	7	4
Hardware	*Laptops*	A	5	9	4	5	4

Àmbit	Actiu	Valor	Aspectes crítics				
			A	C	I	D	T
Aplicacions	Gestor de màquines virtuals	M	4	6	6	8	4
Aplicacions	Sistema operatiu dels servidors	A	6	9	8	7	5
Aplicacions	Software d'adquisició	M	6	3	6	7	5
Aplicacions	Software de publicació	A	4	5	5	8	6
Aplicacions	Software d'emmagatzematge	A	6	7	10	8	3
Aplicacions	Software de processament	M	3	4	7	7	4
Dades	Dades *input* dels estudis	A	7	3	7	4	4
Dades	Dades *output* dels estudis o resultats	MA	5	8	9	7	5
Dades	Credencials d'accés als sistemes	MA	6	10	8	5	4
Dades	Dades personals d'empleats	MA	8	10	8	5	4
Dades	Registres d'activitat	A	5	6	9	5	9
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)	MA	6	9	8	4	5
Dades	Codi font del software propi	A	4	6	9	6	6
Xarxa	Xarxa administrativa	A	7	8	6	7	5
Xarxa	Xarxa interna transferència de dades	MA	4	5	8	8	4
Xarxa	Connexió a Internet - primària	MA	4	4	6	9	3
Xarxa	Connexió a Internet - *backup*	M	4	4	6	6	3
Serveis	Servei de directori	MA	7	7	5	9	4
Serveis	Servei FTP	A	4	3	8	6	3
Serveis	Servei HTTP	A	4	7	5	6	3
Serveis	Servei de correu electrònic	A	6	5	6	6	7
Serveis	Servei d'accés remot o VPN	MA	6	10	5	9	7
Equipament auxiliar	Robot de cintes d'emmagatzematge - primari	A	5	7	10	7	3
Equipament auxiliar	Robot de cintes d'emmagatzematge - *backup*	M	5	7	10	5	3
Equipament auxiliar	Climatització del CPD primari	A	3	3	5	9	3
Equipament auxiliar	Climatització del CPD de *backup*	A	3	3	5	9	3
Equipament auxiliar	Alimentació dels sistemes	A	3	3	5	9	3

Àmbit	Actiu	Valor	Aspectes crítics				
			A	C	I	D	T
Equipament auxiliar	Alimentació dels sistemes - *backup* o *UPS*	A	3	3	5	9	3
Equipament auxiliar	Mobiliari oficines	M	3	6	4	6	3
Equipament auxiliar	Mobiliari sales de reunions	M	3	6	4	6	3
Personal	Administradors de xarxes / subcontractistes	MA	5	8	7	8	3
Personal	Administradors de sistemes / subcontractistes	MA	5	8	7	8	3
Personal	Operadors	MA	5	8	7	8	3
Personal	Desenvolupadors	MA	5	8	7	8	3
Personal	Proveïdors de serveis	MA	5	8	7	8	3

Taula 5: Valoració dels actius de l'Organització

6.4 Anàlisi d'amenaces

En el present apartat cal identificar les amenaces que poden suposar una degradació dels actius de l'Organització, així com definir en quina mesura se'n veuen afectats cadascun dels aspectes crítics. Seguint el procediment establert a l'annex 17. , a continuació es mostra, per a cada actiu rellevant en l'anàlisi de riscos, quina és la probabilitat d'ocurrència de les amenaces (del llistat d'amenaces comuns de Magerit, llibre II [13] al capítol 5) i quin impacte tindria aquesta en cas de materialització sobre cadascuna de les dimensions de seguretat. Cal destacar que s'han contemplat un conjunt d'amenaces que es consideren rellevants i representatives per als actius de l'Organització objecte de l'anàlisi de riscos.

Un factor important a ressaltar per a l'anàlisi d'amenaces és que aquest es realitza tenint en compte l'estat actual de l'Organització. És a dir, considerant que els controls definits a 4.2 estan aplicats.

En l'anàlisi de les degradacions de les amenaces és important abordar les dependències existents entre els actius – veure 6.2 . Així, per a una amenaça que afecti un actiu «inferior», aquesta degradació es veurà reflectida també en els actius «superiors» que es sustentin en el primer. Aquest efecte queda reflectit en les següents taules d'amenaces.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10					
Inundacions, per causes naturals o industrials	1/10					

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Averia de l’equipament o programa (físic o lògic)	n/a					
Tall del subministre elèctric	1					
Averia en el sistema de climatització	1					
Incident en la xarxa de comunicacions	10					
Error d’ús dels sistemes	10		50%	50%	20%	
Error d’administració dels sistemes	10	50%	100%	100%	100%	50%
Incidents deguts a software malintencionat	1		100%	100%	100%	
Alteració de la informació	1	20%		50%		
Destrucció de la informació	1				50%	
Fuga d’informació	1	20%	100%			
Error de manteniment / actualització de software	n/a					
Error de manteniment / actualització de hardware	n/a					
Accés no autoritzat	1	20%				
Intercepció d’informació	1	10%	100%			

Taula 6: Amenaces - actius de Personal

En la taula 6 s’han agrupat els actius de la categoria Personal, ja que les amenaces els afecten de forma similar. Els actius d’aquesta categoria són els únics que actuen exclusivament com a actius «inferiors» dins l’arbre de dependències entre actius de l’Organització. Els actius analitzats a les taules 7 (Instal·lacions) i 8 (Xarxa) constitueixen també la base de la resta d’actius. Aquestes darreres categories, però, poden veure’s afectades pels impactes als actius de la categoria Personal.

Els impactes de les amenaces en els actius de la categoria Personal se centren en com és l’afectació a la informació de les persones. A més de les afectacions directes a la informació (alteració, destrucció i fuga), destaquen les amenaces d’errors en l’administració de sistemes i incidents deguts a software malintencionats. En aquests casos, l’impacte en les dimensions de seguretat de la informació del personal pot ser total.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10			50%	100%	50%
Inundacions, per causes naturals o industrials	1/10			50%	100%	50%
Averia de l’equipament o programa (físic o lògic)	n/a					

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Tall del subministre elèctric	1				50%	
Averia en el sistema de climatització	1			20%	50%	
Incident en la xarxa de comunicacions	10					
Error d'ús dels sistemes	n/a					
Error d'administració dels sistemes	n/a					
Incidents deguts a software malintencionat	n/a					
Alteració de la informació	1	20%		50%		
Destrucció de la informació	1				100%	
Fuga d'informació	1	20%	100%			
Error de manteniment / actualització de software	n/a					
Error de manteniment / actualització de hardware	n/a					
Accés no autoritzat	1	20%	50%	20%		
Intercepció d'informació	n/a					

Taula 7: Amenaces - actius d'Instal·lacions

Les amenaces afecten d'igual forma als dos edificis. És per això que s'analitza el seu impacte mitjançant una única taula.

Com es desprèn de la taula 7, per als actius Edificis, un nombre elevat d'amenaces o bé no tenen cap impacte en els seus aspectes crítics o bé no són d'aplicació (e.g. no té sentit parlar d'error d'actualització de hardware per a un edifici). D'altra banda, hi ha altres amenaces que sí poden afectar aspectes crítics d'aquests actius, com poden ser catàstrofes en forma d'incendi o inundacions, averies elèctriques o de climatització, o accessos no autoritzat a les instal·lacions.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10					
Inundacions, per causes naturals o industrials	1/10					
Averia de l'equipament o programa (físic o lògic)	n/a					
Tall del subministre elèctric	1				50%	
Averia en el sistema de climatització	1					
Incident en la xarxa de comunicacions	10			20%	100%	20%

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Error d’ús dels sistemes	10					
Error d’administració dels sistemes	10	50%	100%	100%	100%	50%
Incidents deguts a software malintencionat	1					
Alteració de la informació	1	20%		100%		
Destrucció de la informació	1				100%	
Fuga d’informació	1	20%	100%			
Error de manteniment / actualització de software	n/a					
Error de manteniment / actualització de hardware	n/a					
Accés no autoritzat	1	20%	50%	50%		
Intercepció d’informació	1		100%			

Taula 8: Amenaces - actius de Xarxa

En la taula 8 s’han agrupat els 4 actius de tipus xarxa, ja que les amenaces els afecten de forma similar. A més de les amenaces de correlació directa, com els incidents en la xarxa de comunicacions, podem destacar amenaces relacionades amb errors d’administració i amb l’alteració, destrucció i fuga d’informació. L’impacte en els actius de totes elles es veu augmentat per la dependència dels actius de tipus Personal.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10			50%	100%	50%
Inundacions, per causes naturals o industrials	1/10			50%	100%	50%
Averia de l’equipament o programa (físic o lògic)	1			20%	100%	
Tall del subministre elèctric	1			20%	100%	
Averia en el sistema de climatització	1				50%	
Incident en la xarxa de comunicacions	10					
Error d’ús dels sistemes	10					
Error d’administració dels sistemes	10	50%	100%	100%	100%	50%
Incidents deguts a software malintencionat	1		100%	100%	100%	
Alteració de la informació	1	20%		50%		
Destrucció de la informació	1				50%	
Fuga d’informació	1	20%	100%			

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Error de manteniment / actualització de software	1				100%	
Error de manteniment / actualització de hardware	1/10				100%	
Accés no autoritzat	1	20%	50%	20%		
Intercepció d’informació	n/a					

Taula 9: Amenaces - actius d’Equipament auxiliar (robots de cintes)

Els actius d'Equipament auxiliar actuen d’actius «superiors» del les Instal·lacions i, com tots els actius de l’Organització, del Personal. Per tant, es veuran afectats per les amenaces que tinguin un impacte en els actius d’aquestes categories. Tal i com s'esmenta a 6.2 , les dependències poden existir per a totes les amenaces o per a un subconjunt de les mateixes.

A l’hora d’analitzar les amenaces que poden degradar el valor dels actius d’Equipament auxiliar s’han realitzat tres taules: 9 (robots de cintes), 10 (climatització i alimentació) i 11 (mobiliari d’oficines i de sales de reunions), ja que l’afectació no és igual per a cadascun dels subgrups.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10			50%	100%	50%
Inundacions, per causes naturals o industrials	1/10			50%	100%	50%
Averia de l’equipament o programa (físic o lògic)	1			20%	100%	
Tall del subministre elèctric	1			20%	100%	
Averia en el sistema de climatització	1				100%	
Incident en la xarxa de comunicacions	10					
Error d’ús dels sistemes	10					
Error d’administració dels sistemes	10				50%	
Incidents deguts a software malintencionat	1					
Alteració de la informació	1			50%		
Destrucció de la informació	1				50%	
Fuga d’informació	1					
Error de manteniment / actualització de software	1					
Error de manteniment / actualització de hardware	1/10				100%	
Accés no autoritzat	1	20%	50%	20%		

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Intercepció d’informació	n/a					

Taula 10: Amenaces - actius d’Equipament auxiliar (climatització i alimentació)

En el cas de l’afectació de les amenaces sobre els actius de climatització i alimentació – taula 10 – aquesta és similar a la reflectida a la taula 9 per al cas dels robots, amb algunes diferències. Una de les més rellevants és la menor afectació en els casos d’errors, tant d’ús com d’administració.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10			50%	100%	50%
Inundacions, per causes naturals o industrials	1/10			50%	100%	50%
Averia de l’equipament o programa (físic o lògic)	n/a					
Tall del subministre elèctric	1					
Averia en el sistema de climatització	1					
Incident en la xarxa de comunicacions	10					
Error d’ús dels sistemes	n/a					
Error d’administració dels sistemes	n/a					
Incidents deguts a software malintencionat	n/a					
Alteració de la informació	1			50%		
Destrucció de la informació	1				50%	
Fuga d’informació	1		50%			
Error de manteniment / actualització de software	n/a					
Error de manteniment / actualització de hardware	n/a					
Accés no autoritzat	1		50%	20%		
Intercepció d’informació	1		50%			

Taula 11: Amenaces - actius d’Equipament auxiliar (mobiliari)

L’últim subgrup dels actius pertanyents a la categoria d’Equipament auxiliar és el mobiliari d’oficines i de sales de reunions. En aquest cas – taula 11 – només algunes amenaces afectarien al valor dels actius. En aquests casos, a més, l’afectació és deguda a la dependència amb els actius de les categories Instal·lacions i Personal.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10			50%	100%	50%
Inundacions, per causes naturals o industrials	1/10			50%	100%	50%
Averia de l'equipament o programa (físic o lògic)	1	20%	50%	50%	100%	20%
Tall del subministre elèctric	1			20%	100%	
Averia en el sistema de climatització	1			20%	100%	
Incident en la xarxa de comunicacions	10			20%	100%	20%
Error d'ús dels sistemes	10					
Error d'administració dels sistemes	10	50%	100%	20%	100%	50%
Incidents deguts a software malintencionat	1		100%	20%	100%	
Alteració de la informació	1	20%		20%		
Destrucció de la informació	1				50%	
Fuga d'informació	1	20%	100%			
Error de manteniment / actualització de software	1		50%		100%	
Error de manteniment / actualització de hardware	1/10		50%		100%	
Accés no autoritzat	1		50%	50%	50%	
Intercepció d'informació	1		100%			

Taula 12: Amenaces - actius de Hardware (routers, switches i tallafocs)

Els actius pertanyents a la categoria Hardware es poden dividir en tres grups, en funció de l'impacte que tindrien la consecució de les diferents amenaces. En conseqüència, s'han creat tres taules per a analitzar les amenaces per a aquesta categoria d'actius de l'Organització: taula 12 (*routers, switches* i tallafocs), taula 13 (servidors) i taula 14 (*laptops*).

Els actius de Hardware es sustenten en els actius «inferiors» de les categories Instal·lacions, Xarxa, Personal i Equipament auxiliar.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10			50%	100%	50%
Inundacions, per causes naturals o industrials	1/10			50%	100%	50%
Averia de l'equipament o programa (físic o lògic)	1	20%	50%	50%	100%	20%

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Tall del subministre elèctric	1			20%	100%	
Averia en el sistema de climatització	1			20%	100%	
Incident en la xarxa de comunicacions	10			20%	100%	20%
Error d'ús dels sistemes	10		100%	20%	100%	
Error d'administració dels sistemes	10	50%	100%	20%	100%	50%
Incidents deguts a software malintencionat	1		100%	20%	100%	
Alteració de la informació	1	20%		50%		
Destrucció de la informació	1				100%	
Fuga d'informació	1	20%	100%			
Error de manteniment / actualització de software	1		50%		100%	
Error de manteniment / actualització de hardware	1/10		50%		100%	
Accés no autoritzat	1		50%	50%	50%	
Intercepció d'informació	1		100%			

Taula 13: Amenaces - actius de Hardware (servidors)

L'anàlisi de l'impacte d'amenaces sobre els actius servidors – taula 13 – és molt similar al realitzat per als actius del primer subgrup de Hardware (*routers*, *switches* i tallafocs) – veure taula 12. Les diferencies recauen, d'una banda, en l'aplicabilitat de l'amenaça d'error d'ús (els servidors sí que s'usen per part de l'equip d'operacions, mentre que els dispositius de xarxa només s'administren) i, d'altra banda, en el grau de degradació de les amenaces d'alteració i destrucció de la informació.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10			50%	100%	50%
Inundacions, per causes naturals o industrials	1/10			50%	100%	50%
Averia de l'equipament o programa (físic o lògic)	1	20%	50%	50%	100%	20%
Tall del subministre elèctric	1			20%	10%	
Averia en el sistema de climatització	1					
Incident en la xarxa de comunicacions	10					
Error d'ús dels sistemes	10	50%	100%	20%	100%	
Error d'administració dels sistemes	10	50%	100%	20%	100%	50%
Incidents deguts a software malintencionat	1		100%	20%	100%	

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Alteració de la informació	1	20%		50%		
Destrucció de la informació	1				100%	
Fuga d'informació	1	20%	100%			
Error de manteniment / actualització de software	1		50%		100%	
Error de manteniment / actualització de hardware	1/10		50%		100%	
Accés no autoritzat	1		50%	50%	50%	
Intercepció d'informació	1		100%			

Taula 14: Amenaces - actius de Hardware (laptops)

En el cas dels *laptops* – taula 14 –, l'anàlisi de l'impacte d'amenaces es pot equiparar al realitzat sobre els servidors – veure taula 13 –, amb algunes diferències: les amenaces de tall de subministre elèctric i de fallida del sistema de climatització no afecten a l'actiu (únicament el cas de tall elèctric de llarga durada, assumint que s'esgota la bateria). D'altra banda, els incidents de comunicacions no afecten l'actiu, mentre que un error en l'ús dels *laptops* afegeix un impacte en la dimensió d'autenticitat.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10					
Inundacions, per causes naturals o industrials	1/10					
Averia de l'equipament o programa (físic o lògic)	1	20%	50%	50%	100%	
Tall del subministre elèctric	1				50%	
Averia en el sistema de climatització	1					
Incident en la xarxa de comunicacions	10			20%	100%	20%
Error d'ús dels sistemes	10		50%	50%	20%	
Error d'administració dels sistemes	10	50%	100%	100%	100%	50%
Incidents deguts a software malintencionat	1	20%	100%	100%	100%	
Alteració de la informació	1	20%		50%		
Destrucció de la informació	1				50%	
Fuga d'informació	1	20%	100%			
Error de manteniment / actualització de software	1		50%		100%	
Error de manteniment / actualització de hardware	n/a					
Accés no autoritzat	1	20%	50%	50%		

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Intercepció d’informació	1	10%	100%			

Taula 15: Amenaces - actius d'Aplicacions

Els actius d’Aplicacions, segons es defineix a la figura 5, actuen com a actius «superiors» dels actius de Xarxa i dels de Personal. Els primers es veuen afectats, doncs, per les degradacions que la consecució d’amenaces provoquen en els segons. A aquestes degradacions acumulades cal afegir les afectacions directes que tenen les amenaces en les aplicacions, com són una avaria de l’aplicació corresponent o un error en el manteniment / actualització del software.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10			50%	100%	50%
Inundacions, per causes naturals o industrials	1/10			50%	100%	50%
Averia de l’equipament o programa (físic o lògic)	1	20%	50%	50%	100%	20%
Tall del subministre elèctric	1			20%	100%	
Averia en el sistema de climatització	1			20%	100%	
Incident en la xarxa de comunicacions	10			20%	100%	20%
Error d’ús dels sistemes	10		100%	50%	100%	
Error d’administració dels sistemes	10	50%	100%	100%	100%	50%
Incidents deguts a software malintencionat	1	20%	100%	100%	100%	
Alteració de la informació	1	20%		50%		
Destrucció de la informació	1				100%	
Fuga d’informació	1	20%	100%			
Error de manteniment / actualització de software	1		50%		100%	
Error de manteniment / actualització de hardware	1/10		50%		100%	
Accés no autoritzat	1	20%	50%	50%	50%	
Intercepció d’informació	1	10%	100%			

Taula 16: Amenaces - actius de Serveis

L’anàlisi de l’impacte de les amenaces sobre els actius de la categoria Serveis es realitza mitjançant una única taula, ja que les amenaces afecten a tots els actius de forma similar. En

el cas dels actius de Serveis, aquests es sustenten en els actius «inferiors» Hardware, Aplicacions i Personal.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Incendi, per causes naturals o industrials	1/10			50%	100%	50%
Inundacions, per causes naturals o industrials	1/10			50%	100%	50%
Averia de l'equipament o programa (físic o lògic)	1	20%	50%	50%	100%	20%
Tall del subministre elèctric	1			20%	100%	
Averia en el sistema de climatització	1			20%	100%	
Incident en la xarxa de comunicacions	10			20%	100%	20%
Error d'ús dels sistemes	10		100%	50%	100%	
Error d'administració dels sistemes	10	50%	100%	100%	100%	50%
Incidents deguts a software malintencionat	1	20%	100%	100%	100%	
Alteració de la informació	1	20%		50%		
Destrucció de la informació	1				100%	
Fuga d'informació	1	20%	100%			
Error de manteniment / actualització de software	1		50%		100%	
Error de manteniment / actualització de hardware	1/10		50%		100%	
Accés no autoritzat	1	20%	50%	50%	50%	
Intercepció d'informació	1	10%	100%			

Taula 17: Amenaces - actius de Dades

Existeixen diversos tipus d'actius en la categoria de Dades, tot ells amb una importància cabdal per als processos de negoci de l'Organització. Tot i la diferent naturalesa dels actius (e.g. les dades d'*input* i *output* dels estudis no tenen res a veure amb les dades personals d'empleats), es poden modelar els impactes de les amenaces sobre aquests de forma similar. Així, es mostren les degradacions en els valors dels actius de Dades en una única taula – veure taula 17.

Els actius de Dades es troben a la part superior de l'arbre de dependències de l'Organització – veure figura 2 –, tenint com a actius «inferiors» els actius de Serveis, d'Aplicacions i de Personal. Si es comparen les taules 16 i 17, s'observa que els impactes que causaran la consecució de les diferents amenaces coincideixen per als actius de Serveis i pels de Dades. La diferència en el càlcul de l'impacte potencial vindrà determinada pel valor de cadascun dels actius – veure 6.3 .

6.5 Avaluacions d’impacte i probabilitats (risc)

Un cop disposem de la valoració dels actius de l’Organització – veure 6.3 – i de l’anàlisi de com afecten les amenaces als mateixos (probabilitat d’ocurrència i grau de degradació) – veure 6.4 –, es calcula ara quin és l’impacte potencial de cadascuna de les amenaces, en el conjunt de l’Organització. Per a fer-ho, i seguint el procediment establert a l’annex 17. , es segueixen els següents passos:

1. Per a cada actiu, calcular l’impacte total com a la suma de les degradacions en els diferents aspectes ACIDT, i respecte als valors de l’actiu. És a dir, com a més valor inicial de l’actiu, més impacte.
2. Considerar els actius «superiors» que, tot i no veure’s afectat directament per l’amenaça, es veuen degradats en el cas que l’actiu «inferior» en el que se sustenten sí estigui afectat. Aquest aspecte ja ha estat considerat en l’anàlisi d’afectació de les amenaces a 6.4 .
3. Agregar els impactes per a cada actiu afectat per l’amenaça, ja sigui de forma directa o indirecte.

Per a cadascuna de les amenaces considerades en el present anàlisi de riscos es realitza una taula implementant els punts anteriors.

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	5	16	7	28
Instal·lacions	Edifici oficines i CPD			2.5	10	3.5	16
Instal·lacions	Edifici CPD de *backup*			2.5	6	3.5	12
Impacte en els actius Hardware		0	0	34	73	30	137
Hardware	*Router* principal - primari			4	9	4	17
Hardware	*Router* principal - *backup*			4	6	4	14
Hardware	*Switches* oficines			2	3	1.5	6.5
Hardware	*Switches* sales de reunions			2	3	1.5	6.5
Hardware	Tallafocs intern (entre la xarxa *backend* de l’Organització i la DMZ)			3	8	4	15
Hardware	Tallafocs extern (entre la DMZ i Internet)			3	10	4	17
Hardware	Servidors d’adquisició (a la DMZ)			3	7	2.5	12.5
Hardware	Servidors de publicació (a la DMZ)			2.5	8	3	13.5
Hardware	Servidors d’emmagatzematge (al *backend*)			5	8	1.5	14.5

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Hardware	Servidors de processament (al *backend*)			3.5	7	2	12.5
Hardware	*Laptops*			2	4	2	8
Impacte en els actius Aplicacions		0	0	0	0	0	0
Aplicacions	Gestor de màquines virtuals						0
Aplicacions	Sistema operatiu dels servidors						0
Aplicacions	Software d'adquisició						0
Aplicacions	Software de publicació						0
Aplicacions	Software d'emmagatzematge						0
Aplicacions	Software de processament						0
Impacte en els actius Dades		0	0	29	36	18.5	83.5
Dades	Dades *input* dels estudis			3.5	4	2	9.5
Dades	Dades *output* dels estudis o resultats			4.5	7	2.5	14
Dades	Credencials d'accés als sistemes			4	5	2	11
Dades	Dades personals d'empleats			4	5	2	11
Dades	Registres d'activitat			4.5	5	4.5	14
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)			4	4	2.5	10.5
Dades	Codi font del software propi			4.5	6	3	13.5
Impacte en els actius Xarxa		0	0	0	0	0	0
Xarxa	Xarxa administrativa						0
Xarxa	Xarxa interna transferència de dades						0
Xarxa	Connexió a Internet - primària						0
Xarxa	Connexió a Internet - *backup*						0
Impacte en els actius Serveis		0	0	14.5	36	12	62.5
Serveis	Servei de directori			2.5	9	2	13.5
Serveis	Servei FTP			4	6	1.5	11.5
Serveis	Servei HTTP			2.5	6	1.5	10
Serveis	Servei de correu electrònic			3	6	3.5	12.5
Serveis	Servei d'accés remot o VPN			2.5	9	3.5	15
Impacte en els actius Equipament auxiliar		0	0	24	60	12	96
E. auxiliar	Robot de cintes d'emmagatzematge - primari			5	7	1.5	13.5
E. auxiliar	Robot de cintes d'emmagatzematge - *backup*			5	5	1.5	11.5
E. auxiliar	Climatització del CPD primari			2.5	9	1.5	13

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
E. auxiliar	Climatització del CPD de *backup*			2.5	9	1.5	13
E. auxiliar	Alimentació dels sistemes			2.5	9	1.5	13
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*			2.5	9	1.5	13
E. auxiliar	Mobiliari oficines			2	6	1.5	9.5
E. auxiliar	Mobiliari sales de reunions			2	6	1.5	9.5
Impacte en els actius Personal		0	0	0	0	0	0
Personal	Administradors de xarxes / subcontractistes						0
Personal	Administradors de sistemes / subcontractistes						0
Personal	Operadors						0
Personal	Desenvolupadors						0
Personal	Proveïdors de serveis						0
Impacte potencial de l’amenaça		**0**	**0**	**106.5**	**221**	**79.5**	**407**

Taula 18: Impacte potencial - amenaça: Incendi

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	5	16	7	28
Instal·lacions	Edifici oficines i CPD			2.5	10	3.5	16
Instal·lacions	Edifici CPD de *backup*			2.5	6	3.5	12
Impacte en els actius Hardware		0	0	34	73	30	137
Hardware	*Router* principal - primari			4	9	4	17
Hardware	*Router* principal - *backup*			4	6	4	14
Hardware	*Switches* oficines			2	3	1.5	6.5
Hardware	*Switches* sales de reunions			2	3	1.5	6.5
Hardware	Tallafocs intern (entre la xarxa *backend* de l’Organització i la DMZ)			3	8	4	15
Hardware	Tallafocs extern (entre la DMZ i Internet)			3	10	4	17
Hardware	Servidors d’adquisició (a la DMZ)			3	7	2.5	12.5
Hardware	Servidors de publicació (a la DMZ)			2.5	8	3	13.5
Hardware	Servidors d’emmagatzematge (al *backend*)			5	8	1.5	14.5
Hardware	Servidors de processament (al *backend*)			3.5	7	2	12.5
Hardware	*Laptops*			2	4	2	8

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Aplicacions		0	0	0	0	0	0
Aplicacions	Gestor de màquines virtuals						0
Aplicacions	Sistema operatiu dels servidors						0
Aplicacions	Software d’adquisició						0
Aplicacions	Software de publicació						0
Aplicacions	Software d’emmagatzematge						0
Aplicacions	Software de processament						0
Impacte en els actius Dades		0	0	29	36	18.5	83.5
Dades	Dades *input* dels estudis			3.5	4	2	9.5
Dades	Dades *output* dels estudis o resultats			4.5	7	2.5	14
Dades	Credencials d’accés als sistemes			4	5	2	11
Dades	Dades personals d’empleats			4	5	2	11
Dades	Registres d’activitat			4.5	5	4.5	14
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)			4	4	2.5	10.5
Dades	Codi font del software propi			4.5	6	3	13.5
Impacte en els actius Xarxa		0	0	0	0	0	0
Xarxa	Xarxa administrativa						0
Xarxa	Xarxa interna transferència de dades						0
Xarxa	Connexió a Internet - primària						0
Xarxa	Connexió a Internet - *backup*						0
Impacte en els actius Serveis		0	0	14.5	36	12	62.5
Serveis	Servei de directori			2.5	9	2	13.5
Serveis	Servei FTP			4	6	1.5	11.5
Serveis	Servei HTTP			2.5	6	1.5	10
Serveis	Servei de correu electrònic			3	6	3.5	12.5
Serveis	Servei d’accés remot o VPN			2.5	9	3.5	15
Impacte en els actius Equipament auxiliar		0	0	24	60	12	96
E. auxiliar	Robot de cintes d’emmagatzematge - primari			5	7	1.5	13.5
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*			5	5	1.5	11.5
E. auxiliar	Climatització del CPD primari			2.5	9	1.5	13
E. auxiliar	Climatització del CPD de *backup*			2.5	9	1.5	13
E. auxiliar	Alimentació dels sistemes			2.5	9	1.5	13

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*			2.5	9	1.5	13
E. auxiliar	Mobiliari oficines			2	6	1.5	9.5
E. auxiliar	Mobiliari sales de reunions			2	6	1.5	9.5
Impacte en els actius Personal		0	0	0	0	0	0
Personal	Administradors de xarxes / subcontractistes						0
Personal	Administradors de sistemes / subcontractistes						0
Personal	Operadors						0
Personal	Desenvolupadors						0
Personal	Proveïdors de serveis						0
Impacte potencial de l'amenaça		**0**	**0**	**106.5**	**221**	**79.5**	**407**

Taula 19: Impacte potencial - amenaça: Inundacions

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	0	0	0	0
Instal·lacions	Edifici oficines i CPD						0
Instal·lacions	Edifici CPD de *backup*						0
Impacte en els actius Hardware		11.6	32	34	74	12	163.6
Hardware	*Router* principal - primari	1	4	4	9	1.6	19.6
Hardware	*Router* principal - *backup*	1	4	4	6	1.6	16.6
Hardware	*Switches* oficines	0.8	3	2	3	0.6	9.4
Hardware	*Switches* sales de reunions	0.8	3	2	3	0.6	9.4
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)	1.6	2	3	8	1.6	16.2
Hardware	Tallafocs extern (entre la DMZ i Internet)	1.6	2	3	10	1.6	18.2
Hardware	Servidors d'adquisició (a la DMZ)	1.2	1.5	3	7	1	13.7
Hardware	Servidors de publicació (a la DMZ)	0.8	2.5	2.5	8	1.2	15
Hardware	Servidors d'emmagatzematge (al *backend*)	1.2	3.5	5	8	0.6	18.3
Hardware	Servidors de processament (al *backend*)	0.6	2	3.5	7	0.8	13.9
Hardware	*Laptops*	1	4.5	2	5	0.8	13.3
Impacte en els actius Aplicacions		5.8	17	21	45	0	88.8
Aplicacions	Gestor de màquines virtuals	0.8	3	3	8		14.8

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Aplicacions	Sistema operatiu dels servidors	1.2	4.5	4	7		16.7
Aplicacions	Software d'adquisició	1.2	1.5	3	7		12.7
Aplicacions	Software de publicació	0.8	2.5	2.5	8		13.8
Aplicacions	Software d'emmagatzematge	1.2	3.5	5	8		17.7
Aplicacions	Software de processament	0.6	2	3.5	7		13.1
Impacte en els actius Dades		8.2	26	29	36	5	104.2
Dades	Dades *input* dels estudis	1.4	1.5	3.5	4	0,8	10.4
Dades	Dades *output* dels estudis o resultats	1	4	4.5	7	1	17.5
Dades	Credencials d'accés als sistemes	1.2	5	4	5	0,8	15.2
Dades	Dades personals d'empleats	1.6	5	4	5	0,8	15.6
Dades	Registres d'activitat	1	3	4.5	5	1.8	15.3
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)	1.2	4.5	4	4	1	14.7
Dades	Codi font del software propi	0.8	3	4.5	6	1.2	15.5
Impacte en els actius Xarxa		0	0	0	0	0	0
Xarxa	Xarxa administrativa						0
Xarxa	Xarxa interna transferència de dades						0
Xarxa	Connexió a Internet - primària						0
Xarxa	Connexió a Internet - *backup*						0
Impacte en els actius Serveis		5.4	16	14.5	36	4.8	76.7
Serveis	Servei de directori	1.4	3.5	2.5	9	0.8	17.2
Serveis	Servei FTP	0.8	1.5	4	6	0.6	12.9
Serveis	Servei HTTP	0.8	3.5	2.5	6	0.6	13.4
Serveis	Servei de correu electrònic	1.2	2.5	3	6	1.4	14.1
Serveis	Servei d'accés remot o VPN	1.2	5	2.5	9	1.4	19.1
Impacte en els actius Equipament auxiliar		0	0	8	48	0	56
E. auxiliar	Robot de cintes d'emmagatzematge - primari			2	7		9
E. auxiliar	Robot de cintes d'emmagatzematge - *backup*			2	5		7
E. auxiliar	Climatització del CPD primari			1	9		10
E. auxiliar	Climatització del CPD de *backup*			1	9		10
E. auxiliar	Alimentació dels sistemes			1	9		10
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*			1	9		10
E. auxiliar	Mobiliari oficines						0

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
E. auxiliar	Mobiliari sales de reunions						0
Impacte en els actius Personal		0	0	0	0	0	0
Personal	Administradors de xarxes / subcontractistes						0
Personal	Administradors de sistemes / subcontractistes						0
Personal	Operadors						0
Personal	Desenvolupadors						0
Personal	Proveïdors de serveis						0
Impacte potencial de l'amenaça		**31**	**91**	**106.5**	**239**	**21.8**	**489.3**

Taula 20: Impacte potencial - amenaça: Averia de l'equipament o programa (físic o lògic)

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	0	8	0	8
Instal·lacions	Edifici oficines i CPD				5		5
Instal·lacions	Edifici CPD de *backup*				3		3
Impacte en els actius Hardware		0	0	13.6	69.5	0	83.1
Hardware	*Router* principal - primari			1.6	9		10.6
Hardware	*Router* principal - *backup*			1.6	6		7.6
Hardware	*Switches* oficines			0.8	3		3.8
Hardware	*Switches* sales de reunions			0.8	3		3.8
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)			1.2	8		9.2
Hardware	Tallafocs extern (entre la DMZ i Internet)			1.2	10		11.2
Hardware	Servidors d'adquisició (a la DMZ)			1.2	7		8.2
Hardware	Servidors de publicació (a la DMZ)			1	8		9
Hardware	Servidors d'emmagatzematge (al *backend*)			2	8		10
Hardware	Servidors de processament (al *backend*)			1.4	7		8.4
Hardware	*Laptops*			0.8	0.5		1.3
Impacte en els actius Aplicacions		0	0	0	22.5	0	22.5
Aplicacions	Gestor de màquines virtuals				4		4
Aplicacions	Sistema operatiu dels servidors				3.5		3.5
Aplicacions	Software d'adquisició				3.5		3.5

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Aplicacions	Software de publicació				4		4
Aplicacions	Software d’emmagatzematge				4		4
Aplicacions	Software de processament				3.5		3.5
Impacte en els actius Dades		0	0	11.6	36	0	47.6
Dades	Dades *input* dels estudis			1.4	4		5.4
Dades	Dades *output* dels estudis o resultats			1.8	7		8.8
Dades	Credencials d’accés als sistemes			1.6	5		6.6
Dades	Dades personals d’empleats			1.6	5		6.6
Dades	Registres d’activitat			1.8	5		6.8
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)			1.6	4		5.6
Dades	Codi font del software propi			1.8	6		7.8
Impacte en els actius Xarxa		0	0	0	15	0	15
Xarxa	Xarxa administrativa				3.5		3.5
Xarxa	Xarxa interna transferència de dades				4		4
Xarxa	Connexió a Internet - primària				4.5		4.5
Xarxa	Connexió a Internet - *backup*				3		3
Impacte en els actius Serveis		0	0	5.8	36	0	41.8
Serveis	Servei de directori			1	9		10
Serveis	Servei FTP			1.6	6		7.6
Serveis	Servei HTTP			1	6		7
Serveis	Servei de correu electrònic			1.2	6		7.2
Serveis	Servei d’accés remot o VPN			1	9		10
Impacte en els actius Equipament auxiliar		0	0	8	48	0	56
E. auxiliar	Robot de cintes d’emmagatzematge - primari			2	7		9
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*			2	5		7
E. auxiliar	Climatització del CPD primari			1	9		10
E. auxiliar	Climatització del CPD de *backup*			1	9		10
E. auxiliar	Alimentació dels sistemes			1	9		10
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*			1	9		10
E. auxiliar	Mobiliari oficines						0
E. auxiliar	Mobiliari sales de reunions						0
Impacte en els actius Personal		0	0	0	0	0	0

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Personal	Administradors de xarxes / subcontractistes						0
Personal	Administradors de sistemes / subcontractistes						0
Personal	Operadors						0
Personal	Desenvolupadors						0
Personal	Proveïdors de serveis						0
Impacte potencial de l'amenaça		**0**	**0**	**39**	**235**	**0**	**274**

Taula 21: Impacte potencial - amenaça: Tall del subministre elèctric

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	2	8	0	10
Instal·lacions	Edifici oficines i CPD			1	5		6
Instal·lacions	Edifici CPD de *backup*			1	3		4
Impacte en els actius Hardware		0	0	12.8	69	0	81.8
Hardware	*Router* principal - primari			1.6	9		10.6
Hardware	*Router* principal - *backup*			1.6	6		7.6
Hardware	*Switches* oficines			0.8	3		3.8
Hardware	*Switches* sales de reunions			0.8	3		3.8
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)			1.2	8		9.2
Hardware	Tallafocs extern (entre la DMZ i Internet)			1.2	10		11.2
Hardware	Servidors d'adquisició (a la DMZ)			1.2	7		8.2
Hardware	Servidors de publicació (a la DMZ)			1	8		9
Hardware	Servidors d'emmagatzematge (al *backend*)			2	8		10
Hardware	Servidors de processament (al *backend*)			1.4	7		8.4
Hardware	*Laptops*						0
Impacte en els actius Aplicacions		0	0	0	0	0	0
Aplicacions	Gestor de màquines virtuals						0
Aplicacions	Sistema operatiu dels servidors						0
Aplicacions	Software d'adquisició						0
Aplicacions	Software de publicació						0
Aplicacions	Software d'emmagatzematge						0

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Aplicacions	Software de processament						0
Impacte en els actius Dades		0	0	11.6	36	0	47.6
Dades	Dades *input* dels estudis			1.4	4		5.4
Dades	Dades *output* dels estudis o resultats			1.8	7		8.8
Dades	Credencials d'accés als sistemes			1.6	5		6.6
Dades	Dades personals d'empleats			1.6	5		6.6
Dades	Registres d'activitat			1.8	5		6.8
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)			1.6	4		5.6
Dades	Codi font del software propi			1.8	6		7.8
Impacte en els actius Xarxa		0	0	0	0	0	0
Xarxa	Xarxa administrativa						0
Xarxa	Xarxa interna transferència de dades						0
Xarxa	Connexió a Internet - primària						0
Xarxa	Connexió a Internet - *backup*						0
Impacte en els actius Serveis		0	0	5.8	36	0	41.8
Serveis	Servei de directori			1	9		10
Serveis	Servei FTP			1.6	6		7.6
Serveis	Servei HTTP			1	6		7
Serveis	Servei de correu electrònic			1.2	6		7.2
Serveis	Servei d'accés remot o VPN			1	9		10
Impacte en els actius Equipament auxiliar		0	0	0	42	0	42
E. auxiliar	Robot de cintes d'emmagatzematge - primari				3.5		3.5
E. auxiliar	Robot de cintes d'emmagatzematge - *backup*				2.5		2.5
E. auxiliar	Climatització del CPD primari				9		9
E. auxiliar	Climatització del CPD de *backup*				9		9
E. auxiliar	Alimentació dels sistemes				9		9
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*				9		9
E. auxiliar	Mobiliari oficines						0
E. auxiliar	Mobiliari sales de reunions						0
Impacte en els actius Personal		0	0	0	0	0	0
Personal	Administradors de xarxes / subcontractistes						0
Personal	Administradors de sistemes / subcontractistes						0

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Personal	Operadors						0
Personal	Desenvolupadors						0
Personal	Proveïdors de serveis						0
Impacte potencial de l'amenaça		**0**	**0**	**32.2**	**191**	**0**	**223.2**

Taula 22: Impacte potencial - amenaça: Averia en el sistema de climatització

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	0	0	0	0
Instal·lacions	Edifici oficines i CPD						0
Instal·lacions	Edifici CPD de *backup*						0
Impacte en els actius Hardware		0	0	12.8	69	11.2	93
Hardware	*Router* principal - primari			1.6	9	1.6	12.2
Hardware	*Router* principal - *backup*			1.6	6	1.6	9.2
Hardware	*Switches* oficines			0.8	3	0.6	4.4
Hardware	*Switches* sales de reunions			0.8	3	0.6	4.4
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)			1.2	8	1.6	10.8
Hardware	Tallafocs extern (entre la DMZ i Internet)			1.2	10	1.6	12.8
Hardware	Servidors d'adquisició (a la DMZ)			1.2	7	1	9.2
Hardware	Servidors de publicació (a la DMZ)			1	8	1.2	10.2
Hardware	Servidors d'emmagatzematge (al *backend*)			2	8	0.6	10.6
Hardware	Servidors de processament (al *backend*)			1.4	7	0.8	9.2
Hardware	*Laptops*						0
Impacte en els actius Aplicacions		0	0	8.4	45	5.4	58.8
Aplicacions	Gestor de màquines virtuals			1.2	8	0.8	10
Aplicacions	Sistema operatiu dels servidors			1.6	7	1	9.6
Aplicacions	Software d'adquisició			1.2	7	1	9.2
Aplicacions	Software de publicació			1	8	1.2	10.2
Aplicacions	Software d'emmagatzematge			2	8	0.6	10.6
Aplicacions	Software de processament			1.4	7	0.8	9.2
Impacte en els actius Dades		0	0	11.6	36	7.4	55

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Dades	Dades *input* dels estudis			1.4	4	0.8	6.2
Dades	Dades *output* dels estudis o resultats			1.8	7	1	9.8
Dades	Credencials d’accés als sistemes			1.6	5	0.8	7.4
Dades	Dades personals d’empleats			1.6	5	0.8	7.4
Dades	Registres d’activitat			1.8	5	1.8	8.6
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)			1.6	4	1	6.6
Dades	Codi font del software propi			1.8	6	1.2	9
Impacte en els actius Xarxa		0	0	5.2	30	3	38.2
Xarxa	Xarxa administrativa			1.2	7	1	9.2
Xarxa	Xarxa interna transferència de dades			1.6	8	0.8	10.4
Xarxa	Connexió a Internet - primària			1.2	9	0.6	10.8
Xarxa	Connexió a Internet - *backup*			1.2	6	0.6	7.8
Impacte en els actius Serveis		0	0	5.8	36	4.8	46.6
Serveis	Servei de directori			1	9	0.8	10.8
Serveis	Servei FTP			1.6	6	0.6	8.2
Serveis	Servei HTTP			1	6	0.6	7.6
Serveis	Servei de correu electrònic			1.2	6	1.4	8.6
Serveis	Servei d’accés remot o VPN			1	9	1.4	11.4
Impacte en els actius Equipament auxiliar		0	0	0	0	0	0
E. auxiliar	Robot de cintes d’emmagatzematge - primari						0
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*						0
E. auxiliar	Climatització del CPD primari						0
E. auxiliar	Climatització del CPD de *backup*						0
E. auxiliar	Alimentació dels sistemes						0
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*						0
E. auxiliar	Mobiliari oficines						0
E. auxiliar	Mobiliari sales de reunions						0
Impacte en els actius Personal		0	0	0	0	0	0
Personal	Administradors de xarxes / subcontractistes						0
Personal	Administradors de sistemes / subcontractistes						0
Personal	Operadors						0
Personal	Desenvolupadors						0

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Personal	Proveïdors de serveis						0
Impacte potencial de l'amenaça		**0**	**0**	**43.8**	**216**	**31.8**	**291.6**

Taula 23: Impacte potencial - amenaça: Incident en la xarxa de comunicacions

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	0	0	0	0
Instal·lacions	Edifici oficines i CPD						0
Instal·lacions	Edifici CPD de *backup*						0
Impacte en els actius Hardware		2.5	28	6.4	35	0	71.9
Hardware	*Router* principal - primari						0
Hardware	*Router* principal - *backup*						0
Hardware	*Switches* oficines						0
Hardware	*Switches* sales de reunions						0
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)						0
Hardware	Tallafocs extern (entre la DMZ i Internet)						0
Hardware	Servidors d'adquisició (a la DMZ)		3	1.2	7		11.2
Hardware	Servidors de publicació (a la DMZ)		5	1	8		14
Hardware	Servidors d'emmagatzematge (al *backend*)		7	2	8		17
Hardware	Servidors de processament (al *backend*)		4	1.4	7		12.4
Hardware	*Laptops*	2.5	9	0.8	5		17.3
Impacte en els actius Aplicacions		0	17	21	9	0	47
Aplicacions	Gestor de màquines virtuals		3	3	1.6		7.6
Aplicacions	Sistema operatiu dels servidors		4.5	4	1.4		9.9
Aplicacions	Software d'adquisició		1.5	3	1.4		5.9
Aplicacions	Software de publicació		2.5	2.5	1.6		6.6
Aplicacions	Software d'emmagatzematge		3.5	5	1.6		10.1
Aplicacions	Software de processament		2	3.5	1.4		6.9
Impacte en els actius Dades		0	52	29	36	0	117
Dades	Dades *input* dels estudis		3	3.5	4		10.5
Dades	Dades *output* dels estudis o resultats		8	4.5	7		19.5

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Dades	Credencials d’accés als sistemes		10	4	5		19
Dades	Dades personals d’empleats		10	4	5		19
Dades	Registres d’activitat		6	4.5	5		15.5
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)		9	4	4		17
Dades	Codi font del software propi		6	4.5	6		16.5
Impacte en els actius Xarxa		0	0	0	0	0	0
Xarxa	Xarxa administrativa						0
Xarxa	Xarxa interna transferència de dades						0
Xarxa	Connexió a Internet - primària						0
Xarxa	Connexió a Internet - *backup*						0
Impacte en els actius Serveis		0	32	14.5	36	0	82.5
Serveis	Servei de directori		7	2.5	9		18.5
Serveis	Servei FTP		3	4	6		13
Serveis	Servei HTTP		7	2.5	6		15.5
Serveis	Servei de correu electrònic		5	3	6		14
Serveis	Servei d’accés remot o VPN		10	2.5	9		21.5
Impacte en els actius Equipament auxiliar		0	0	0	0	0	0
E. auxiliar	Robot de cintes d’emmagatzematge - primari						0
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*						0
E. auxiliar	Climatització del CPD primari						0
E. auxiliar	Climatització del CPD de *backup*						0
E. auxiliar	Alimentació dels sistemes						0
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*						0
E. auxiliar	Mobiliari oficines						0
E. auxiliar	Mobiliari sales de reunions						0
Impacte en els actius Personal		0	20	17.5	8	0	45.5
Personal	Administradors de xarxes / subcontractistes		4	3.5	1.6		9.1
Personal	Administradors de sistemes / subcontractistes		4	3.5	1.6		9.1
Personal	Operadors		4	3.5	1.6		9.1
Personal	Desenvolupadors		4	3.5	1.6		9.1
Personal	Proveïdors de serveis		4	3.5	1.6		9.1
Impacte potencial de l’amenaça		**2.5**	**149**	**88.4**	**124**	**0**	**363.9**

Taula 24: Impacte potencial - amenaça: Error d'ús dels sistemes

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	0	0	0	0
Instal·lacions	Edifici oficines i CPD						0
Instal·lacions	Edifici CPD de *backup*						0
Impacte en els actius Hardware		29	64	13.6	74	30	210.6
Hardware	*Router* principal - primari	2.5	8	1.6	9	4	25.1
Hardware	*Router* principal - *backup*	2.5	8	1.6	6	4	22.1
Hardware	*Switches* oficines	2	6	0.8	3	1.5	13.3
Hardware	*Switches* sales de reunions	2	6	0.8	3	1.5	13.3
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)	4	4	1.2	8	4	21.2
Hardware	Tallafocs extern (entre la DMZ i Internet)	4	4	1.2	10	4	23.2
Hardware	Servidors d'adquisició (a la DMZ)	3	3	1.2	7	2.5	16.7
Hardware	Servidors de publicació (a la DMZ)	2	5	1	8	3	19
Hardware	Servidors d'emmagatzematge (al *backend*)	3	7	2	8	1.5	21.5
Hardware	Servidors de processament (al *backend*)	1.5	4	1.4	7	2	15.9
Hardware	*Laptops*	2.5	9	0.8	5	2	19.3
Impacte en els actius Aplicacions		14.5	34	42	45	13.5	149
Aplicacions	Gestor de màquines virtuals	2	6	6	8	2	24
Aplicacions	Sistema operatiu dels servidors	3	9	8	7	2.5	29.5
Aplicacions	Software d'adquisició	3	3	6	7	2.5	21.5
Aplicacions	Software de publicació	2	5	5	8	3	23
Aplicacions	Software d'emmagatzematge	3	7	10	8	1.5	29.5
Aplicacions	Software de processament	1.5	4	7	7	2	21.5
Impacte en els actius Dades		20.5	52	58	36	18.5	185
Dades	Dades *input* dels estudis	3.5	3	7	4	2	19.5
Dades	Dades *output* dels estudis o resultats	2.5	8	9	7	2.5	29
Dades	Credencials d'accés als sistemes	3	10	8	5	2	28
Dades	Dades personals d'empleats	4	10	8	5	2	29
Dades	Registres d'activitat	2.5	6	9	5	4.5	27
Dades	Dades contractuals (amb proveïdors de	3	9	8	4	2.5	26.5

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
	serveis i terceres entitats)						
Dades	Codi font del software propi	2	6	9	6	3	26
Impacte en els actius Xarxa		9.5	21	26	30	7.5	94
Xarxa	Xarxa administrativa	3.5	8	6	7	2.5	27
Xarxa	Xarxa interna transferència de dades	2	5	8	8	2	25
Xarxa	Connexió a Internet - primària	2	4	6	9	1.5	22.5
Xarxa	Connexió a Internet - *backup*	2	4	6	6	1.5	19.5
Impacte en els actius Serveis		13.5	32	29	36	12	122.5
Serveis	Servei de directori	3.5	7	5	9	2	26.5
Serveis	Servei FTP	2	3	8	6	1.5	20.5
Serveis	Servei HTTP	2	7	5	6	1.5	21.5
Serveis	Servei de correu electrònic	3	5	6	6	3.5	23.5
Serveis	Servei d’accés remot o VPN	3	10	5	9	3.5	30.5
Impacte en els actius Equipament auxiliar		5	14	20	30	3	72
E. auxiliar	Robot de cintes d’emmagatzematge - primari	2.5	7	10	7	1.5	28
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*	2.5	7	10	5	1.5	26
E. auxiliar	Climatització del CPD primari				4.5		4.5
E. auxiliar	Climatització del CPD de *backup*				4.5		4.5
E. auxiliar	Alimentació dels sistemes				4.5		4.5
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*				4.5		4.5
E. auxiliar	Mobiliari oficines						0
E. auxiliar	Mobiliari sales de reunions						0
Impacte en els actius Personal		12.5	40	35	40	7.5	135
Personal	Administradors de xarxes / subcontractistes	2.5	8	7	8	1.5	27
Personal	Administradors de sistemes / subcontractistes	2.5	8	7	8	1.5	27
Personal	Operadors	2.5	8	7	8	1.5	27
Personal	Desenvolupadors	2.5	8	7	8	1.5	27
Personal	Proveïdors de serveis	2.5	8	7	8	1.5	27
Impacte potencial de l’amenaça		**104.5**	**257**	**223.6**	**291**	**92**	**968.1**

Taula 25: Impacte potencial - amenaça: Error d’administració dels sistemes

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	0	0	0	0
Instal·lacions	Edifici oficines i CPD						0
Instal·lacions	Edifici CPD de *backup*						0
Impacte en els actius Hardware		0	64	13.6	74	0	151.6
Hardware	*Router* principal - primari		8	1.6	9		18.6
Hardware	*Router* principal - *backup*		8	1.6	6		15.6
Hardware	*Switches* oficines		6	0.8	3		9.8
Hardware	*Switches* sales de reunions		6	0.8	3		9.8
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)		4	1.2	8		13.2
Hardware	Tallafocs extern (entre la DMZ i Internet)		4	1.2	10		15.2
Hardware	Servidors d'adquisició (a la DMZ)		3	1.2	7		11.2
Hardware	Servidors de publicació (a la DMZ)		5	1	8		14
Hardware	Servidors d'emmagatzematge (al *backend*)		7	2	8		17
Hardware	Servidors de processament (al *backend*)		4	1.4	7		12.4
Hardware	*Laptops*		9	0.8	5		14.8
Impacte en els actius Aplicacions		5.8	34	42	45	0	126.8
Aplicacions	Gestor de màquines virtuals	0.8	6	6	8		20.8
Aplicacions	Sistema operatiu dels servidors	1.2	9	8	7		25.2
Aplicacions	Software d'adquisició	1.2	3	6	7		17.2
Aplicacions	Software de publicació	0.8	5	5	8		18.8
Aplicacions	Software d'emmagatzematge	1.2	7	10	8		26.2
Aplicacions	Software de processament	0.6	4	7	7		18.6
Impacte en els actius Dades		8.2	52	58	36	0	154.2
Dades	Dades *input* dels estudis	1.4	3	7	4		15.4
Dades	Dades *output* dels estudis o resultats	1	8	9	7		25
Dades	Credencials d'accés als sistemes	1.2	10	8	5		24.2
Dades	Dades personals d'empleats	1.6	10	8	5		24.6
Dades	Registres d'activitat	1	6	9	5		21
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)	1.2	9	8	4		22.2
Dades	Codi font del software propi	0.8	6	9	6		21.8
Impacte en els actius Xarxa		0	0	0	0	0	0

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Xarxa	Xarxa administrativa						0
Xarxa	Xarxa interna transferència de dades						0
Xarxa	Connexió a Internet - primària						0
Xarxa	Connexió a Internet - *backup*						0
Impacte en els actius Serveis		5.4	32	29	36	0	102.4
Serveis	Servei de directori	1.4	7	5	9		22.4
Serveis	Servei FTP	0.8	3	8	6		17.8
Serveis	Servei HTTP	0.8	7	5	6		18.8
Serveis	Servei de correu electrònic	1.2	5	6	6		18.2
Serveis	Servei d’accés remot o VPN	1.2	10	5	9		25.2
Impacte en els actius Equipament auxiliar		0	14	20	12	0	46
E. auxiliar	Robot de cintes d’emmagatzematge - primari		7	10	7		24
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*		7	10	5		22
E. auxiliar	Climatització del CPD primari						0
E. auxiliar	Climatització del CPD de *backup*						0
E. auxiliar	Alimentació dels sistemes						0
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*						0
E. auxiliar	Mobiliari oficines						0
E. auxiliar	Mobiliari sales de reunions						0
Impacte en els actius Personal		0	40	35	40	0	115
Personal	Administradors de xarxes / subcontractistes		8	7	8		23
Personal	Administradors de sistemes / subcontractistes		8	7	8		23
Personal	Operadors		8	7	8		23
Personal	Desenvolupadors		8	7	8		23
Personal	Proveïdors de serveis		8	7	8		23
Impacte potencial de l’amenaça		**19.4**	**236**	**197.6**	**243**	**0**	**696**

Taula 26: Impacte potencial - amenaça: Incidents deguts a software malintencionat

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		1.6	0	5	0	0	6.6
Instal·lacions	Edifici oficines i CPD	0.8		2.5			3.3

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Instal·lacions	Edifici CPD de *backup*	0.8		2.5			3.3
Impacte en els actius Hardware		11.6	0	23.2	0	0	34.8
Hardware	*Router* principal - primari	1		1.6			2.6
Hardware	*Router* principal - *backup*	1		1.6			2.6
Hardware	*Switches* oficines	0.8		0.8			1.6
Hardware	*Switches* sales de reunions	0.8		0.8			1.6
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)	1.6		1.2			2.8
Hardware	Tallafocs extern (entre la DMZ i Internet)	1.6		1.2			2.8
Hardware	Servidors d'adquisició (a la DMZ)	1.2		3			4.2
Hardware	Servidors de publicació (a la DMZ)	0.8		2.5			3.3
Hardware	Servidors d'emmagatzematge (al *backend*)	1.2		5			6.2
Hardware	Servidors de processament (al *backend*)	0.6		3.5			4.1
Hardware	*Laptops*	1		2			3
Impacte en els actius Aplicacions		5.8	0	21	0	0	26.8
Aplicacions	Gestor de màquines virtuals	0.8		3			3.8
Aplicacions	Sistema operatiu dels servidors	1.2		4			5.2
Aplicacions	Software d'adquisició	1.2		3			4.2
Aplicacions	Software de publicació	0.8		2.5			3.3
Aplicacions	Software d'emmagatzematge	1.2		5			6.2
Aplicacions	Software de processament	0.6		3.5			4.1
Impacte en els actius Dades		8.2	0	29	0	0	37.2
Dades	Dades *input* dels estudis	1.4		3.5			4.9
Dades	Dades *output* dels estudis o resultats	1		4.5			5.5
Dades	Credencials d'accés als sistemes	1.2		4			5.2
Dades	Dades personals d'empleats	1.6		4			5.6
Dades	Registres d'activitat	1		4.5			5.5
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)	1.2		4			5.2
Dades	Codi font del software propi	0.8		4.5			5.3
Impacte en els actius Xarxa		3.8	0	26	0	0	29.8
Xarxa	Xarxa administrativa	1.4		6			7.4
Xarxa	Xarxa interna transferència de dades	0.8		8			8.8

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Xarxa	Connexió a Internet - primària	0.8		6			6.8
Xarxa	Connexió a Internet - *backup*	0.8		6			6.8
Impacte en els actius Serveis		5.4	0	14.5	0	0	19.9
Serveis	Servei de directori	1.4		2.5			3.9
Serveis	Servei FTP	0.8		4			4.8
Serveis	Servei HTTP	0.8		2.5			3.3
Serveis	Servei de correu electrònic	1.2		3			4.2
Serveis	Servei d’accés remot o VPN	1.2		2.5			3.7
Impacte en els actius Equipament auxiliar		2	0	24	0	0	26
E. auxiliar	Robot de cintes d’emmagatzematge - primari	1		5			6
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*	1		5			6
E. auxiliar	Climatització del CPD primari			2.5			2.5
E. auxiliar	Climatització del CPD de *backup*			2.5			2.5
E. auxiliar	Alimentació dels sistemes			2.5			2.5
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*			2.5			2.5
E. auxiliar	Mobiliari oficines			2			2
E. auxiliar	Mobiliari sales de reunions			2			2
Impacte en els actius Personal		5	0	17.5	0	0	22.5
Personal	Administradors de xarxes / subcontractistes	1		3.5			4.5
Personal	Administradors de sistemes / subcontractistes	1		3.5			4.5
Personal	Operadors	1		3.5			4.5
Personal	Desenvolupadors	1		3.5			4.5
Personal	Proveïdors de serveis	1		3.5			4.5
Impacte potencial de l’amenaça		**43.4**	**0**	**160.2**	**0**	**0**	**203.6**

Taula 27: Impacte potencial - amenaça: Alteració de la informació

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	0	16	0	16
Instal·lacions	Edifici oficines i CPD				10		10
Instal·lacions	Edifici CPD de *backup*				6		6
Impacte en els actius Hardware		0	0	0	54.5	0	54.5

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Hardware	*Router* principal - primari				4.5		4.5
Hardware	*Router* principal - *backup*				3		3
Hardware	*Switches* oficines				1.5		1.5
Hardware	*Switches* sales de reunions				1.5		1.5
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)				4		4
Hardware	Tallafocs extern (entre la DMZ i Internet)				5		5
Hardware	Servidors d'adquisició (a la DMZ)				7		7
Hardware	Servidors de publicació (a la DMZ)				8		8
Hardware	Servidors d'emmagatzematge (al *backend*)				8		8
Hardware	Servidors de processament (al *backend*)				7		7
Hardware	*Laptops*				5		5
Impacte en els actius Aplicacions		0	0	0	22.5	0	22.5
Aplicacions	Gestor de màquines virtuals				4		4
Aplicacions	Sistema operatiu dels servidors				3.5		3.5
Aplicacions	Software d'adquisició				3.5		3.5
Aplicacions	Software de publicació				4		4
Aplicacions	Software d'emmagatzematge				4		4
Aplicacions	Software de processament				3.5		3.5
Impacte en els actius Dades		0	0	0	36	0	36
Dades	Dades *input* dels estudis				4		4
Dades	Dades *output* dels estudis o resultats				7		7
Dades	Credencials d'accés als sistemes				5		5
Dades	Dades personals d'empleats				5		5
Dades	Registres d'activitat				5		5
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)				4		4
Dades	Codi font del software propi				6		6
Impacte en els actius Xarxa		0	0	0	30	0	30
Xarxa	Xarxa administrativa				7		7
Xarxa	Xarxa interna transferència de dades				8		8
Xarxa	Connexió a Internet - primària				9		9
Xarxa	Connexió a Internet - *backup*				6		6

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Serveis		0	0	0	36	0	36
Serveis	Servei de directori				9		9
Serveis	Servei FTP				6		6
Serveis	Servei HTTP				6		6
Serveis	Servei de correu electrònic				6		6
Serveis	Servei d’accés remot o VPN				9		9
Impacte en els actius Equipament auxiliar		0	0	0	30	0	30
E. auxiliar	Robot de cintes d’emmagatzematge - primari				3.5		3.5
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*				2.5		2.5
E. auxiliar	Climatització del CPD primari				4.5		4.5
E. auxiliar	Climatització del CPD de *backup*				4.5		4.5
E. auxiliar	Alimentació dels sistemes				4.5		4.5
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*				4.5		4.5
E. auxiliar	Mobiliari oficines				3		3
E. auxiliar	Mobiliari sales de reunions				3		3
Impacte en els actius Personal		0	0	0	20	0	20
Personal	Administradors de xarxes / subcontractistes				4		4
Personal	Administradors de sistemes / subcontractistes				4		4
Personal	Operadors				4		4
Personal	Desenvolupadors				4		4
Personal	Proveïdors de serveis				4		4
Impacte potencial de l’amenaça		**0**	**0**	**0**	**245**	**0**	**245**

Taula 28: Impacte potencial - amenaça: Destrucció de la informació

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		1.6	10	0	0	0	11.6
Instal·lacions	Edifici oficines i CPD	0.8	5				5.8
Instal·lacions	Edifici CPD de *backup*	0.8	5				5.8
Impacte en els actius Hardware		11.6	64	0	0	0	75.6
Hardware	*Router* principal - primari	1	8				9
Hardware	*Router* principal - *backup*	1	8				9

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Hardware	*Switches* oficines	0.8	6				6.8
Hardware	*Switches* sales de reunions	0.8	6				6.8
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)	1.6	4				5.6
Hardware	Tallafocs extern (entre la DMZ i Internet)	1.6	4				5.6
Hardware	Servidors d'adquisició (a la DMZ)	1.2	3				4.2
Hardware	Servidors de publicació (a la DMZ)	0.8	5				5.8
Hardware	Servidors d'emmagatzematge (al *backend*)	1.2	7				8.2
Hardware	Servidors de processament (al *backend*)	0.6	4				4.6
Hardware	*Laptops*	1	9				10
Impacte en els actius Aplicacions		5.8	34	0	0	0	39.8
Aplicacions	Gestor de màquines virtuals	0.8	6				6.8
Aplicacions	Sistema operatiu dels servidors	1.2	9				10.2
Aplicacions	Software d'adquisició	1.2	3				4.2
Aplicacions	Software de publicació	0.8	5				5.8
Aplicacions	Software d'emmagatzematge	1.2	7				8.2
Aplicacions	Software de processament	0.6	4				4.6
Impacte en els actius Dades		8.2	52	0	0	0	60.2
Dades	Dades *input* dels estudis	1.4	3				4.4
Dades	Dades *output* dels estudis o resultats	1	8				9
Dades	Credencials d'accés als sistemes	1.2	10				11.2
Dades	Dades personals d'empleats	1.6	10				11.6
Dades	Registres d'activitat	1	6				7
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)	1.2	9				10.2
Dades	Codi font del software propi	0.8	6				6.8
Impacte en els actius Xarxa		3.8	21	0	0	0	24.8
Xarxa	Xarxa administrativa	1.4	8				9.4
Xarxa	Xarxa interna transferència de dades	0.8	5				5.8
Xarxa	Connexió a Internet - primària	0.8	4				4.8
Xarxa	Connexió a Internet - *backup*	0.8	4				4.8
Impacte en els actius Serveis		5.4	32	0	0	0	37.4
Serveis	Servei de directori	1.4	7				8.4

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Serveis	Servei FTP	0.8	3				3.8
Serveis	Servei HTTP	0.8	7				7.8
Serveis	Servei de correu electrònic	1.2	5				6.2
Serveis	Servei d’accés remot o VPN	1.2	10				11.2
Impacte en els actius	Equipament auxiliar	2	20	0	0	0	22
E. auxiliar	Robot de cintes d’emmagatzematge - primari	1	7				8
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*	1	7				8
E. auxiliar	Climatització del CPD primari						0
E. auxiliar	Climatització del CPD de *backup*						0
E. auxiliar	Alimentació dels sistemes						0
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*						0
E. auxiliar	Mobiliari oficines		3				3
E. auxiliar	Mobiliari sales de reunions		3				3
Impacte en els actius	Personal	5	40	0	0	0	45
Personal	Administradors de xarxes / subcontractistes	1	8				9
Personal	Administradors de sistemes / subcontractistes	1	8				9
Personal	Operadors	1	8				9
Personal	Desenvolupadors	1	8				9
Personal	Proveïdors de serveis	1	8				9
Impacte potencial de l’amenaça		**43.4**	**273**	**0**	**0**	**0**	**316.4**

Taula 29: Impacte potencial - amenaça: Fuga d’informació

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius	Instal·lacions	0	0	0	0	0	0
Instal·lacions	Edifici oficines i CPD						0
Instal·lacions	Edifici CPD de *backup*						0
Impacte en els actius	Hardware	0	32	0	74	0	106
Hardware	*Router* principal - primari		4		9		13
Hardware	*Router* principal - *backup*		4		6		10
Hardware	*Switches* oficines		3		3		6
Hardware	*Switches* sales de reunions		3		3		6

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)		2		8		10
Hardware	Tallafocs extern (entre la DMZ i Internet)		2		10		12
Hardware	Servidors d'adquisició (a la DMZ)		1.5		7		8.5
Hardware	Servidors de publicació (a la DMZ)		2.5		8		10.5
Hardware	Servidors d'emmagatzematge (al *backend*)		3.5		8		11.5
Hardware	Servidors de processament (al *backend*)		2		7		9
Hardware	*Laptops*		4.5		5		9.5
Impacte en els actius Aplicacions		0	17	0	45	0	62
Aplicacions	Gestor de màquines virtuals		3		8		11
Aplicacions	Sistema operatiu dels servidors		4.5		7		11.5
Aplicacions	Software d'adquisició		1.5		7		8.5
Aplicacions	Software de publicació		2.5		8		10.5
Aplicacions	Software d'emmagatzematge		3.5		8		11.5
Aplicacions	Software de processament		2		7		9
Impacte en els actius Dades		0	26	0	36	0	62
Dades	Dades *input* dels estudis		1.5		4		5.5
Dades	Dades *output* dels estudis o resultats		4		7		11
Dades	Credencials d'accés als sistemes		5		5		10
Dades	Dades personals d'empleats		5		5		10
Dades	Registres d'activitat		3		5		8
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)		4.5		4		8.5
Dades	Codi font del software propi		3		6		9
Impacte en els actius Xarxa		0	0	0	0	0	0
Xarxa	Xarxa administrativa						0
Xarxa	Xarxa interna transferència de dades						0
Xarxa	Connexió a Internet - primària						0
Xarxa	Connexió a Internet - *backup*						0
Impacte en els actius Serveis		0	16	0	36	0	52
Serveis	Servei de directori		3.5		9		12.5
Serveis	Servei FTP		1.5		6		7.5
Serveis	Servei HTTP		3.5		6		9.5

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Serveis	Servei de correu electrònic		2.5		6		8.5
Serveis	Servei d'accés remot o VPN		5		9		14
Impacte en els actius Equipament auxiliar		0	0	0	12	0	12
E. auxiliar	Robot de cintes d'emmagatzematge - primari				7		7
E. auxiliar	Robot de cintes d'emmagatzematge - *backup*				5		5
E. auxiliar	Climatització del CPD primari						0
E. auxiliar	Climatització del CPD de *backup*						0
E. auxiliar	Alimentació dels sistemes						0
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*						0
E. auxiliar	Mobiliari oficines						0
E. auxiliar	Mobiliari sales de reunions						0
Impacte en els actius Personal		0	0	0	0	0	0
Personal	Administradors de xarxes / subcontractistes						0
Personal	Administradors de sistemes / subcontractistes						0
Personal	Operadors						0
Personal	Desenvolupadors						0
Personal	Proveïdors de serveis						0
Impacte potencial de l'amenaça		**0**	**91**	**0**	**203**	**0**	**294**

Taula 30: Impacte potencial - amenaça: Error de manteniment / actualització de software

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	0	0	0	0
Instal·lacions	Edifici oficines i CPD						0
Instal·lacions	Edifici CPD de *backup*						0
Impacte en els actius Hardware		0	32	0	74	0	106
Hardware	*Router* principal - primari		4		9		13
Hardware	*Router* principal - *backup*		4		6		10
Hardware	*Switches* oficines		3		3		6
Hardware	*Switches* sales de reunions		3		3		6
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)		2		8		10

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Hardware	Tallafocs extern (entre la DMZ i Internet)		2		10		12
Hardware	Servidors d'adquisició (a la DMZ)		1.5		7		8.5
Hardware	Servidors de publicació (a la DMZ)		2.5		8		10.5
Hardware	Servidors d'emmagatzematge (al *backend*)		3.5		8		11.5
Hardware	Servidors de processament (al *backend*)		2		7		9
Hardware	*Laptops*		4.5		5		9.5
Impacte en els actius Aplicacions		0	0	0	0	0	0
Aplicacions	Gestor de màquines virtuals						0
Aplicacions	Sistema operatiu dels servidors						0
Aplicacions	Software d'adquisició						0
Aplicacions	Software de publicació						0
Aplicacions	Software d'emmagatzematge						0
Aplicacions	Software de processament						0
Impacte en els actius Dades		0	26	0	36	0	62
Dades	Dades *input* dels estudis		1.5		4		5.5
Dades	Dades *output* dels estudis o resultats		4		7		11
Dades	Credencials d'accés als sistemes		5		5		10
Dades	Dades personals d'empleats		5		5		10
Dades	Registres d'activitat		3		5		8
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)		4.5		4		8.5
Dades	Codi font del software propi		3		6		9
Impacte en els actius Xarxa		0	0	0	0	0	0
Xarxa	Xarxa administrativa						0
Xarxa	Xarxa interna transferència de dades						0
Xarxa	Connexió a Internet - primària						0
Xarxa	Connexió a Internet - *backup*						0
Impacte en els actius Serveis		0	16	0	36	0	52
Serveis	Servei de directori		3.5		9		12.5
Serveis	Servei FTP		1.5		6		7.5
Serveis	Servei HTTP		3.5		6		9.5
Serveis	Servei de correu electrònic		2.5		6		8.5
Serveis	Servei d'accés remot o VPN		5		9		14

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Equipament auxiliar		0	0	0	48	0	48
E. auxiliar	Robot de cintes d'emmagatzematge - primari				7		7
E. auxiliar	Robot de cintes d'emmagatzematge - *backup*				5		5
E. auxiliar	Climatització del CPD primari				9		9
E. auxiliar	Climatització del CPD de *backup*				9		9
E. auxiliar	Alimentació dels sistemes				9		9
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*				9		9
E. auxiliar	Mobiliari oficines						0
E. auxiliar	Mobiliari sales de reunions						0
Impacte en els actius Personal		0	0	0	0	0	0
Personal	Administradors de xarxes / subcontractistes						0
Personal	Administradors de sistemes / subcontractistes						0
Personal	Operadors						0
Personal	Desenvolupadors						0
Personal	Proveïdors de serveis						0
Impacte potencial de l'amenaça		**0**	**74**	**0**	**194**	**0**	**268**

Taula 31: Impacte potencial - amenaça: Error de manteniment / actualització de hardware

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		1.6	5	2	0	0	8.6
Instal·lacions	Edifici oficines i CPD	0.8	2.5	1			4.3
Instal·lacions	Edifici CPD de *backup*	0.8	2.5	1			4.3
Impacte en els actius Hardware		0	32	34	37	0	103
Hardware	*Router* principal - primari		4	4	4.5		12.5
Hardware	*Router* principal - *backup*		4	4	3		11
Hardware	*Switches* oficines		3	2	1.5		6.5
Hardware	*Switches* sales de reunions		3	2	1.5		6.5
Hardware	Tallafocs intern (entre la xarxa *backend* de l'Organització i la DMZ)		2	3	4		9
Hardware	Tallafocs extern (entre la DMZ i Internet)		2	3	5		10
Hardware	Servidors d'adquisició (a la DMZ)		1.5	3	3.5		8

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Hardware	Servidors de publicació (a la DMZ)		2.5	2.5	4		9
Hardware	Servidors d'emmagatzematge (al *backend*)		3.5	5	4		12.5
Hardware	Servidors de processament (al *backend*)		2	3.5	3.5		9
Hardware	*Laptops*		4.5	2	2.5		9
Impacte en els actius Aplicacions		5.8	17	21	0	0	43.8
Aplicacions	Gestor de màquines virtuals	0.8	3	3			6.8
Aplicacions	Sistema operatiu dels servidors	1.2	4.5	4			9.7
Aplicacions	Software d'adquisició	1.2	1.5	3			5.7
Aplicacions	Software de publicació	0.8	2.5	2.5			5.8
Aplicacions	Software d'emmagatzematge	1.2	3.5	5			9.7
Aplicacions	Software de processament	0.6	2	3.5			6.1
Impacte en els actius Dades		8.2	26	29	18	0	81.2
Dades	Dades *input* dels estudis	1.4	1.5	3.5	2		8.4
Dades	Dades *output* dels estudis o resultats	1	4	4.5	3.5		13
Dades	Credencials d'accés als sistemes	1.2	5	4	2.5		12.7
Dades	Dades personals d'empleats	1.6	5	4	2.5		13.1
Dades	Registres d'activitat	1	3	4.5	2.5		11
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)	1.2	4.5	4	2		11.7
Dades	Codi font del software propi	0.8	3	4.5	3		11.3
Impacte en els actius Xarxa		3.8	10.5	13	0	0	27.3
Xarxa	Xarxa administrativa	1.4	4	3			8.4
Xarxa	Xarxa interna transferència de dades	0.8	2.5	4			7.3
Xarxa	Connexió a Internet - primària	0.8	2	3			5.8
Xarxa	Connexió a Internet - *backup*	0.8	2	3			5.8
Impacte en els actius Serveis		5.4	16	14.5	18	0	53.9
Serveis	Servei de directori	1.4	3.5	2.5	4.5		11.9
Serveis	Servei FTP	0.8	1.5	4	3		9.3
Serveis	Servei HTTP	0.8	3.5	2.5	3		9.8
Serveis	Servei de correu electrònic	1.2	2.5	3	3		9.7
Serveis	Servei d'accés remot o VPN	1.2	5	2.5	4.5		13.2
Impacte en els actius Equipament auxiliar		4.4	19	9.6	0	0	33
E. auxiliar	Robot de cintes d'emmagatzematge - primari	1	3.5	2			6.5

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
E. auxiliar	Robot de cintes d’emmagatzematge - *backup*	1	3.5	2			6.5
E. auxiliar	Climatització del CPD primari	0.6	1.5	1			3.1
E. auxiliar	Climatització del CPD de *backup*	0.6	1.5	1			3.1
E. auxiliar	Alimentació dels sistemes	0.6	1.5	1			3.1
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*	0.6	1.5	1			3.1
E. auxiliar	Mobiliari oficines		3	0.8			3.8
E. auxiliar	Mobiliari sales de reunions		3	0.8			3.8
Impacte en els actius Personal		5	0	0	0	0	5
Personal	Administradors de xarxes / subcontractistes	1					1
Personal	Administradors de sistemes / subcontractistes	1					1
Personal	Operadors	1					1
Personal	Desenvolupadors	1					1
Personal	Proveïdors de serveis	1					1
Impacte potencial de l’amenaça		**34.2**	**125.5**	**123.1**	**73**	**0**	**355.8**

Taula 32: Impacte potencial - amenaça: Accés no autoritzat

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Impacte en els actius Instal·lacions		0	0	0	0	0	0
Instal·lacions	Edifici oficines i CPD						0
Instal·lacions	Edifici CPD de *backup*						0
Impacte en els actius Hardware		0	64	0	0	0	64
Hardware	*Router* principal - primari		8				8
Hardware	*Router* principal - *backup*		8				8
Hardware	*Switches* oficines		6				6
Hardware	*Switches* sales de reunions		6				6
Hardware	Tallafocs intern (entre la xarxa *backend* de l’Organització i la DMZ)		4				4
Hardware	Tallafocs extern (entre la DMZ i Internet)		4				4
Hardware	Servidors d’adquisició (a la DMZ)		3				3
Hardware	Servidors de publicació (a la DMZ)		5				5
Hardware	Servidors d’emmagatzematge (al *backend*)		7				7

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
Hardware	Servidors de processament (al *backend*)		4				4
Hardware	*Laptops*		9				9
Impacte en els actius Aplicacions		2.9	34	0	0	0	36.9
Aplicacions	Gestor de màquines virtuals	0.4	6				6.4
Aplicacions	Sistema operatiu dels servidors	0.6	9				9.6
Aplicacions	Software d'adquisició	0.6	3				3.6
Aplicacions	Software de publicació	0.4	5				5.4
Aplicacions	Software d'emmagatzematge	0.6	7				7.6
Aplicacions	Software de processament	0.3	4				4.3
Impacte en els actius Dades		4.1	52	0	0	0	56.1
Dades	Dades *input* dels estudis	0.7	3				3.7
Dades	Dades *output* dels estudis o resultats	0.5	8				8.5
Dades	Credencials d'accés als sistemes	0.6	10				10.6
Dades	Dades personals d'empleats	0.8	10				10.8
Dades	Registres d'activitat	0.5	6				6.5
Dades	Dades contractuals (amb proveïdors de serveis i terceres entitats)	0.6	9				9.6
Dades	Codi font del software propi	0.4	6				6.4
Impacte en els actius Xarxa		0	21	0	0	0	21
Xarxa	Xarxa administrativa		8				8
Xarxa	Xarxa interna transferència de dades		5				5
Xarxa	Connexió a Internet - primària		4				4
Xarxa	Connexió a Internet - *backup*		4				4
Impacte en els actius Serveis		2.7	32	0	0	0	34.7
Serveis	Servei de directori	0.7	7				7.7
Serveis	Servei FTP	0.4	3				3.4
Serveis	Servei HTTP	0.4	7				7.4
Serveis	Servei de correu electrònic	0.6	5				5.6
Serveis	Servei d'accés remot o VPN	0.6	10				10.6
Impacte en els actius Equipament auxiliar		0	6	0	0	0	6
E. auxiliar	Robot de cintes d'emmagatzematge - primari						0
E. auxiliar	Robot de cintes d'emmagatzematge - *backup*						0
E. auxiliar	Climatització del CPD primari						0

Àmbit	Actiu	Aspectes crítics					Impacte total
		A	C	I	D	T	
E. auxiliar	Climatització del CPD de *backup*						0
E. auxiliar	Alimentació dels sistemes						0
E. auxiliar	Alimentació dels sistemes - *backup* o *UPS*						0
E. auxiliar	Mobiliari oficines		3				3
E. auxiliar	Mobiliari sales de reunions		3				3
Impacte en els actius Personal		2.5	40	0	0	0	42.5
Personal	Administradors de xarxes / subcontractistes	0.5	8				8.5
Personal	Administradors de sistemes / subcontractistes	0.5	8				8.5
Personal	Operadors	0.5	8				8.5
Personal	Desenvolupadors	0.5	8				8.5
Personal	Proveïdors de serveis	0.5	8				8.5
Impacte potencial de l'amenaça		**12.2**	**249**	**0**	**0**	**0**	**261.2**

Taula 33: Impacte potencial - amenaça: Intercepció d'informació

De les taules anteriors – veure taula 18 a taula 33 –, i coneixent les probabilitats d'ocurrència de les diferents amenaces, podem calcular el risc associat a cadascuna d'elles. Per a fer-ho, es multiplica l'impacte potencial de cada amenaça amb la freqüència associada a la mateixa, tal i com es mostra a la taula 77. A més, i com s'especifica al requisit 8.2.1 de la norma ISO/IEC 27001 [3], es defineix un propietari responsable de cadascun dels riscos.

Amenaça	Impacte potencial	Vulnerabilitat o freqüència	Risc	Propietari del risc
Incendi, per causes naturals o industrials	407	1/10	40.7	*IT Manager*
Inundacions, per causes naturals o industrials	407	1/10	40.7	*IT Manager*
Averia de l'equipament o programa (físic o lògic)	489.3	1	489.3	*IT Manager*
Tall del subministre elèctric	274	1	274	*IT Manager*
Averia en el sistema de climatització	223.2	1	223.2	*IT Manager*
Incident en la xarxa de comunicacions	291.6	10	2916	*IT Manager*
Error d'ús dels sistemes	363.9	10	3639	CISO
Error d'administració dels sistemes	968.1	10	9681	CISO
Incidents deguts a software malintencionat	696	1	696	CISO
Alteració de la informació	203.6	1	203.6	CISO

Amenaça	Impacte potencial	Vulnerabilitat o freqüència	Risc	Propietari del risc
Destrucció de la informació	245	1	245	CISO
Fuga d'informació	316.4	1	316.4	CISO
Error de manteniment / actualització de software	294	1	294	*IT Manager*
Error de manteniment / actualització de hardware	268	1/10	26.8	*IT Manager*
Accés no autoritzat	355.8	1	355.8	CISO
Intercepció d'informació	261.2	1	261.2	CISO

Taula 34: Risc de les amenaces

De la taula anterior es desprèn que les amenaces que suposen un risc més elevat per als processos de negoci de l'Organització són les relacionades amb errors d'ús o d'administració dels sistemes i les que tenen a veure amb incidents en la xarxa de comunicacions. Aquest risc tant superior en comparació amb les altres amenaces ve principalment determinat per l'elevada probabilitat d'ocurrència (o vulnerabilitat o freqüència). D'altra banda, les amenaces amb una probabilitat d'ocurrència més baixa són, alhora, les que suposen un menor risc per a l'Organització: incendi, inundacions i errors de manteniment / actualització de hardware.

La possible mitigació dels riscos existents es tracta en altres capítols del present document – veure 7. .

Tal i com s'esmenta a 6.4 , l'anàlisi d'amenaces s'ha realitzat tenint en consideració els controls de seguretats ja establerts en els processos de l'Organització – veure 4.2 . Per tant, els riscos associats a les amenaces calculats a la taula 34 es poden considerar riscos residuals respecte als controls existents actualment l'Organització.

7. Proposta de projectes

L'etapa de proposta de projectes, entesa com a element fonamental del pla director de la seguretat de l'Organització, adquireix rellevància un cop es disposa d'informació sobre l'estat de la seguretat de l'Organització. Això és, tan bon punt s'han realitzat els anàlisis de compliment inicial, tant de la norma ISO/IEC 27001 [3] – veure 4.1 – com dels controls definits a l'ISO/IEC 27002 [1] – veure 4.2 –, així com l'anàlisi de riscos – veure 6. . Un cop es coneix l'estat actual de la seguretat de la informació, i quins són els aspectes que poden (i cal) millorar, es defineixen un conjunt de projectes amb aquesta finalitat de millora. En concret, les propostes de projectes recollides en el present apartat persegueixen un o més dels següents objectius:

- Mitigar el risc actual a l'Organització, segons ha estat aquest identificat a 6. .
- Millorar el compliment de la norma ISO/IEC 27001, tal i com s'ha analitzat a 4.1 .
- Millorar el compliment dels controls ISO/IEC 27002, tal i com s'ha analitzat a 4.2 .

Per a cadascuna de les propostes de projectes presentades a continuació s'inclou, a més d'una descripció del projecte i de les diferents fases o activitats principals que el componen, una planificació temporal de les mateixes i una valoració econòmica per assolir-ne els objectius. En quant a la millora potencial que suposa cada projecte sobre l'SGSI de l'Organització, s'indicarà quin o quins riscos / requisits de la norma ISO/IEC 27001 / controls ISO/IEC 27002 es veuen millorats i, si s'escau, en quina mesura. Així doncs, les propostes de projectes contindran els següents elements:

- **Descripció del projecte**: Es tracta d'una breu descripció de la proposta. Amb aquesta informació ha de quedar clar quina és la naturalesa del projecte així com la seva motivació principal.

- **Fases del projecte**: Apartat que conté les diferents fases en les que es pot descompondre el projecte de millora. Per a cada fase, cal incloure'n la planificació temporal (en general, curt, mig i llarg termini) i els recursos necessaris per a dur-la a terme. En quant a la valoració econòmica i per motius de confidencialitat, es pressuposa un cost genèric de 25€/hora per al personal de l'Organització i de 50€/hora per a proveïdors de serveis, subcontractistes i altres tercers. Un altre motiu de la generalització del cost associat al treball és el de simplificar el càlcul de la despesa econòmica associada al projecte, tal i com es va realitzar en activitats d'assignatures relacionades amb el present treball de màster – veure [5].

- **Millora del risc de l'Organització**: Quin o quins riscos, dels identificats a 6. , es veuen mitigats gràcies a la implementació de la proposta de projecte. Aquest apartat no és d'aplicació obligatòria per a cada proposta.

- **Millora del compliment de la norma ISO/IEC 27001**: Quin o quins requisits de la norma es veuen millorats, respecte a l'estat exposat a 4.1 . Sempre que sigui possible, cal definir quin és el grau de millora. Aquest apartat no és d'aplicació obligatòria per a cada proposta.

- **Millora del compliment dels controls ISO/IEC 27002**: Quin o quins controls es veuen millorats, respecte a l'estat exposat a 4.2 . Sempre que sigui possible, cal definir quin és el grau de millora. Aquest apartat no és d'aplicació obligatòria per a cada proposta.

Un cop disposem de l'avaluació de les millores aportades per les diferents propostes de projectes sobre l'SGSI de l'Organització, es realitza un anàlisi de l'impacte que tenen totes elles en conjunt. Per a fer-ho, i respecte a l'evolució del compliment de la norma ISO/IEC 27001 i els controls ISO/IEC 27002, es mostra com han augmentat els nivells de maduresa dels diferents elements i com aquests representen una millora en els anàlisi GAP corresponents. En quant al riscos residuals de l'Organització, es mostra en quina mesura aquests es veuen reduïts.

7.1 Projecte 1: Campanyes de difusió i conscienciació sobre seguretat de la informació a l'Organització

El present projecte contempla el disseny i execució de campanyes informatives sobre seguretat de la informació. Els receptors de les campanyes són tots els empleats de l'Organització, així com proveïdors de serveis, subcontractistes i altres tercers que participin, de forma directa o indirecte, en els processos de negoci de l'Organització.

La finalitat principal de les campanyes és la conscienciació de tota persona implicada en els processos de l'Organització sobre temàtiques relacionades amb la seguretat de la informació. D'igual manera, les activitats contemplades en el projecte també han de perseguir l'objectiu de distribuir tota aquella documentació de l'SGSI que sigui de domini públic i que, segons el que s'estableix als estàndards ISO/IEC 27001 i ISO/IEC 27002, ha de ser posada en coneixement de totes les parts interessades i de tota l'Organització (e.g. la política de seguretat o altres polítiques o reglaments).

7.1.1 Fases del projecte

Es consideren les següents fases en les quals es pot descompondre el present projecte.

Reunions inicials per avaluar l'estat actual:

Es tracta de reunions en les quals, d'una banda, es mira d'obtenir l'estat actual de tota la documentació de la qual se n'haurà de fer difusió (e.g. les diferents polítiques i reglaments de seguretat). D'altra banda, es discuteixen i es prenen decisions sobre quina o quines són les alternatives més adequades per a dur a terme les campanyes de conscienciació (e.g. a través de correu electrònic, amb presentacions virtuals, amb presentacions físiques, duent a terme seminaris, etc).

Els participants necessaris d'aquesta primera fase del projecte, juntament amb el conjunt d'hores estimades, es veuen recollits en la següent taula.

Personal	# hores internes	# hores externes
Directiu	8	
CISO	16	
IT Manager	8	

Taula 35: Cost estimat - projecte 1: fase inicial

Del conjunt d'hores pressupostades a la taula 35, obtenim que la valoració econòmica de la present fase és de **800 €**.

Els objectius de les reunions i avaluacions inicials es poden programar amb un horitzó temporal de **curt termini**.

Preparació del material per a les campanyes de conscienciació:

Un cop s'ha decidit l'estratègia a seguir a l'hora de dur a terme les campanyes, caldrà preparar-ne el material. Aquest pot ésser de naturalesa variada, com: diapositives, documentació escrita, o material per seminaris virtuals o presencials. Amb la finalitat d'abastar tota la casuística esmentada, s'assumeix que hi haurà, com a mínim, una campanya de cada tipus.

En quant als documents relacionats amb la seguretat de la informació pertanyents a l'Organització, assumim que no hi ha cap cost de preparació. Les tasques d'elaboració i revisió de la documentació no formen part de les activitats del present projecte.

Els participants necessaris per a la fase de preparació del material, juntament amb el conjunt d'hores estimades, es veuen recollits en la següent taula.

Personal	# hores internes	# hores externes
Directiu	4	
CISO	8	
Treballador de l'àrea de seguretat de la informació	24	
IT Manager	4	
Treballador de l'àrea d'IT	24	
Consultor extern (preparació seminaris presencials)		16

Taula 36: Cost estimat - projecte 1: preparació de material

Del conjunt d'hores pressupostades a la taula 36, obtenim que la valoració econòmica de la present fase és de **2.400 €**.

La preparació de tots els materials necessaris per a dur a terme les campanyes de conscienciació és una activitat a planificar entre **curt i mig termini**. Cal destacar, a més, que serà necessari revisar el material en el futur (e.g. pot ésser necessari adaptar-lo o estendre'l). Així doncs, la fase actual té també una dimensió d'activitat a **llarg termini**.

Execució de les campanyes:

En aquesta darrera fase del projecte es duen a terme totes aquelles activitats planificades amb anterioritat, fent ús del material preparat i les sessions organitzades. A l'hora d'afrontar el càlcul del cost estimat, és necessari considerar tant el personal necessari per a la realització de les campanyes – aquell personal que «dona» la informació – com tot aquell temps invertit per a «rebre» la informació i assimilar-la, per part de tots els empleats de l'Organització, així com proveïdors de serveis, subcontractistes i altres tercers.

Els participants necessaris per a la fase d'execució de les campanyes, juntament amb el conjunt d'hores estimades, es veuen recollits en la següent taula.

Personal	# hores internes	# hores externes
Directiu	8	
CISO	8	
IT Manager	8	

Personal	# hores internes	# hores externes
Consultor extern (execució seminaris presencials)		24
Treballadors de totes les àrees (2 hores per campanyes i 1 hora per documentació)	600	
Proveïdors de serveis		24
Altres tercers		16

Taula 37: Cost estimat - projecte 1: execució de campanyes

Del conjunt d'hores pressupostades a la taula 37, obtenim que la valoració econòmica de la present fase és de **18.800 €**.

L'execució de les diferents campanyes de seguretat i la difusió i assimilació de la documentació de l'Organització són activitats que es duran a terme de forma continuada. Per aquest motiu, i degut a que seran necessàries repeticions periòdiques de les campanyes, es pot programar aquesta fase amb un horitzó temporal de **mig i llarg termini**.

7.1.2 Millora del risc

Els riscos associats als processos de negoci de l'Organització, en el cas d'aplicació del present projecte, es veurien afectats de la següent forma:

Error d'ús dels sistemes

- ➔ Les campanyes periòdiques de conscienciació i difusió sobre temes de seguretat influirien molt positivament en l'atenció dels empleats, proveïdors de serveis, subcontractistes i altres tercers, a l'hora d'utilitzar els sistemes, reduint així la freqüència d'ocurrència de l'amenaça.
- ➔ La vulnerabilitat o freqüència es redueix a 1.

Error d'administració dels sistemes

- ➔ De forma similar al cas d'ús dels sistemes, les campanyes aconsegueixen l'objectiu de reduir els errors d'administració de sistemes.
- ➔ La vulnerabilitat o freqüència es redueix a 1.

Incidents deguts a software malintencionat

- ➔ Tant les campanyes que eduquen sobre com tractar amb el software, com el coneixement d'aquell software permès / no permès (control A.12.6.2), aconsegueixen reduir la probabilitat d'ocurrència de l'amenaça.
- ➔ La vulnerabilitat o freqüència es redueix a 1/10.

Alteració de la informació

- ➔ Les campanyes de conscienciació possibiliten una gestió adequada dels sistemes i, al seu torn, redueixen events d'alteració de la informació.
- ➔ La vulnerabilitat o freqüència es redueix a 1/10.

Destrucció de la informació

- ➔ Les campanyes de conscienciació possibiliten una gestió adequada dels sistemes i, al seu torn, redueixen events de destrucció de la informació.
- ➔ La vulnerabilitat o freqüència es redueix a 1/10.

Fuga d'informació

- ➔ Les campanyes de conscienciació possibiliten una gestió adequada dels sistemes i, al seu torn, redueixen events de fuga d'informació.
- ➔ La vulnerabilitat o freqüència es redueix a 1/10.

Intercepció d'informació

- ➔ Les campanyes de conscienciació possibiliten una gestió adequada dels sistemes. Aquest fet permet reduir la probabilitat d'intercepció d'informació, ja sigui per un millor ús dels sistemes o una millor configuració i administració dels mateixos.
- ➔ La vulnerabilitat o freqüència es redueix a 1/10.

7.1.3 Millora del compliment de la norma ISO/IEC 27001

Els requisits de la norma ISO/IEC 27001 que es veurien millorats per l'aplicació del present projecte són:

5.2.3: S'ha comunicat la política de seguretat de la informació a les parts interessades i a tota l'empresa?

- ➔ La política de seguretat s'ha donat a conèixer a tota la empresa i parts implicades.
- ➔ El nivell de maduresa del requisit augmenta a 4.

5.3.2: S'han comunicat convenientment les responsabilitats i les autoritats per a la Seguretat de la Informació?

- ➔ Les responsabilitats i autoritats en matèria de seguretat de la informació han estat definides en el present pla director de seguretat – veure 5.5 i l'annex 16. .
- ➔ Aquesta informació es dona a conèixer a tota la empresa i parts implicades.
- ➔ El nivell de maduresa del requisit augmenta a 4.

7.3.1: El personal està involucrat i és conscient del seu paper a la Seguretat de la Informació?

- ➔ Les campanyes de conscienciació aconsegueixen que tot el personal de l'Organització (i altres parts implicades com e.g. els proveïdors de serveis) siguin conscients del seu paper a la Seguretat de la Informació.
- ➔ El nivell de maduresa del requisit augmenta a 4.

7.3.2: Hi ha consciència dels danys que es poden produir de no seguir les pautes de la Seguretat de la Informació?

- ➔ Un dels objectius de les campanyes de conscienciació és destacar la importància de les mesures de seguretat i, en conseqüència, els perjudicis del no compliment de les mateixes.
- ➔ El nivell de maduresa del requisit augmenta a 4.

7.4.1: Es comunica la política de la Seguretat de la Informació amb les responsabilitats de cadascú?

- ➔ La política de seguretat – incloent les responsabilitats de cada rol – s'ha donat a conèixer a tota la empresa i parts implicades.
- ➔ El nivell de maduresa del requisit augmenta a 4.

7.4.2: Hi ha un procés per comunicar les deficiències o males pràctiques en la seguretat de la informació?

- ➔ S'ha redactat un procediment sobre comunicacions dins de l'Organització – veure annex 12. –, el qual inclou el procés de comunicació de deficiències o males pràctiques.
- ➔ El nivell de maduresa del requisit augmenta a 4.

Requisits 5.2.1, 5.2.2, 5.2.4, 5.3.1, 7.5.1, 7.5.2

- ➔ Aquests requisits es veuen millorats pel present projecte, de forma indirecta, ja que és necessària la existència de la documentació a la que fan referència, per tal de poder dur a terme campanyes educatives al respecte.

7.1.4 Millora del compliment dels controls ISO/IEC 27002

Els controls ISO/IEC 27002 que es veurien millorats per l'aplicació del present projecte són:

A.7.2.1: Responsabilitats de gestió

- ➔ La comunicació periòdica de les responsabilitats en matèria de seguretat a tota la empresa i parts implicades millora el compliment de les mateixes.
- ➔ El nivell de maduresa del control augmenta a 4.

A.7.2.2: Conscienciació, educació i capacitació en seguretat de la informació

- ➔ Un dels principals objectius del present projecte és precisament la conscienciació, educació i capacitació en seguretat de la informació.
- ➔ El nivell de maduresa del control augmenta a 4.

A.11.2.3: Seguretat del cablejat

- ➔ Les campanyes aconsegueixen, entre d'altres, millorar l'estat del cablejat, ja sigui en els despatxos o en els CPDs.
- ➔ El nivell de maduresa del control augmenta a 4.

A.11.2.8: Equip d'usuari desatès

- ➔ La millora, en aquest cas, fa referència principalment als usuaris finals, és a dir, als treballadors o contractistes. Les campanyes de conscienciació aconsegueixen millorar les mesures preses a l'hora de protegir equips desatesos.
- ➔ El nivell de maduresa del control augmenta a 4.

A.12.6.2: Restricció en la instal·lació de software

- ➔ La documentació comunicada inclou aquelles polítiques relacionades amb el software permès / no permès.
- ➔ El nivell de maduresa del control augmenta a 4.

A.16.1.2: Notificació dels events de seguretat de la informació

- ➔ Les campanyes de conscienciació fan èmfasi, entre d'altres, en la notificació d'events de seguretat de la informació.
- ➔ El nivell de maduresa del control augmenta a 4.

A.16.1.3: Notificació de punts dèbils de la seguretat

- ➔ Similar a A.16.1.2, incloent la notificació dels punts dèbils detectats.
- ➔ El nivell de maduresa del control augmenta a 4.

Controls A.5.1.1, A.6.1.1, A.6.1.2, A.6.2.1, A.6.2.2, A.8.1.3, A.10.1.1, A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4, A.15.1.1, A.15.1.2, A.16.1.1

- ➔ Aquests controls es veuen millorats pel present projecte, de forma indirecta, ja que és necessària la existència de la documentació a la que fan referència, per tal de poder dur a terme campanyes educatives al respecte.

7.2 Projecte 2: Implementació i gestió d'indicadors dels controls de seguretat

La finalitat principal del present projecte és millorar el nivell de maduresa dels diferents controls de seguretat que apliquen a l'Organització en l'àmbit de seguretat de la informació – veure annex 18. . Gràcies a la implementació dels indicadors definits a l'annex 14. , i a una gestió continuada dels mateixos, entesa com a seguiment, mesurament, anàlisi i avaluació, serà possible assolir un nivell de maduresa 4 dels controls de seguretat (GESTIONAT I MESURABLE), requisit previ al nivell 5 (OPTIMITZAT).

El present projecte contempla, doncs, l'anàlisi de les activitats i recursos necessaris per a implementar i gestionar els indicadors. Un cop identificades les tasques i assignats els recursos, cal executar les activitats conforme a la planificació.

7.2.1 Fases del projecte

Es consideren les següents fases en les quals es pot descompondre el present projecte.

Reunions inicials per definir les tasques i recursos necessaris:

Es tracta de reunions del grup de treball, en les quals s'han d'analitzar i definir quines són les tasques que caldrà dur a terme per a implementar els indicadors, segons aquests han estat establerts. Les activitats també hauran de contemplar les revisions periòdiques que es duran a terme un cop els indicadors ja han estat implementats i com a part de la fase de monitorització i revisió constant de l'SGSI. En aquesta fase, a més, també caldrà definir quin són els recursos necessaris per a la correcte consecució de totes les activitats proposades.

Els participants necessaris d'aquesta primera fase del projecte, juntament amb el conjunt d'hores estimades, es veuen recollits en la següent taula.

Personal	# hores internes	# hores externes
Directiu	16	
CISO	16	
IT Manager	8	
Consultor extern expert en ISO/IEC 27000		8
Treballadors de RRHH	4	

Taula 38: Cost estimat - projecte 2: definició de tasques i recursos

Del conjunt d'hores pressupostades a la taula 38, obtenim que la valoració econòmica de la present fase és de **1500 €**.

Els objectius de les reunions i avaluacions inicials es poden programar amb un horitzó temporal de **curt termini**.

Implementació dels indicadors de seguretat:

La segona fase del present projecte te com a objectiu principal la implementació dels indicadors de seguretat, tal i com estan definits a l'annex 14. , i per part d'aquells empleats als quals se'ls hi ha designat la tasca (i assignat els recursos per a fer-ho).

El personal que es veu involucrat en aquesta fase d'implementació, juntament amb el conjunt d'hores estimades, es veuen recollits en la següent taula. En quant a l'implementació de mesures tècniques (e.g. eines de monitoratge d'accés), cal esmentar que aquestes ja existeixen i estan plenament operatives. Així doncs, no es considera cap cost afegit en aquest sentit.

Personal	# hores internes	# hores externes
Directiu	12	
CISO	24	
IT Manager	12	
Treballadors de RRHH	4	
Responsable de desenvolupament	1	
Responsable d'operacions	1	
Responsable de qualitat	1	

Taula 39: Cost estimat - projecte 2: implementació dels indicadors

Del conjunt d'hores pressupostades a la taula 39, obtenim que la valoració econòmica de la present fase és de **1.375 €**.

Les activitats per implementar els diferents indicadors de seguretat es poden planificar a **curt termini**.

Gestió continuada dels indicadors de seguretat:

La fase de gestió continuada dels indicadors, entenent que aquests s'han de mesurar, analitzar i avaluar de forma periòdica, és la fase del present projecte que, clarament, requereix de més recursos.

Els participants necessaris per aquesta fase, juntament amb el conjunt d'hores estimades, es veuen recollits en la següent taula. Cal destacar que el càlcul de recursos fa referència a les

hores anuals necessàries. És a dir, és un nou cost recurrent que tindrà l'Organització un cop els indicadors hagin estat implementats.

Personal	# hores internes	# hores externes
Directiu	36	
CISO	150	
IT Manager	63	
Treballadors de RRHH	4	
Responsable de desenvolupament	4	
Responsable d'operacions	4	
Responsable de qualitat	4	

Taula 40: Cost estimat - projecte 2: gestió dels indicadors

Del conjunt d'hores pressupostades a la taula 40, obtenim que la valoració econòmica de la present fase – recordem, de forma anual – és de **6.625 €**.

La planificació temporal de les activitats pertanyents a la fase de gestió d'indicadors abasta un horitzó temporal molt ampli: les activitats han de començar tant bon punt els indicadors estiguin implementats i, al seu torn, la gestió es durà a terme de forma continua i indefinidament, sempre i quan la direcció de l'Organització mantingui els recursos necessaris associats. Podem dir, doncs, que aquesta fase del projecte es pot planificar a **curt, mig i llarg termini**.

7.2.2 Millora del risc

Els riscos associats als processos de negoci de l'Organització es veuen beneficiats de forma generalitzada degut a l'aplicació del present projecte.

El fet de disposar ara d'indicadors que permeten avaluar l'efectivitat dels diferents controls de seguretat i, indirectament, que possibiliten una evolució dels mateixos en cas que s'observi un potencial de millora, resulta en una reducció de tots els riscos identificats a 6. . Degut a la dificultat de quantificar el benefici que proporciona un projecte tan transversal, assumim una millora generalitzada del 10%, entenent-se com a una reducció de l'impacte potencial de les diferents amenaces.

7.2.3 Millora del compliment de la norma ISO/IEC 27001

Els requisits de la norma ISO/IEC 27001 que es veurien millorats per l'aplicació del present projecte són:

9.1.1: S'ha establert un procés continu de monitorització dels aspectes clau de la seguretat de la informació tenint en compte els controls per a la seguretat de la informació?

- ➔ La implantació i la gestió dels indicadors de seguretat possibiliten una monitorització continua dels aspectes clau de la seguretat de la informació.
- ➔ El nivell de maduresa del requisit augmenta a 4.

9.1.2: S'ha establert un procés documentat per avaluar els resultats dels mesuraments i que aquests resultats són presos en compte pels responsables tant dels processos com de la Seguretat de la informació?

- ➔ Els indicadors, en la seva descripció a l'annex 14. , inclouen quina és la manera d'avaluar-los i quins en són els llindars. A més, també existeixen rols i grups de treball específics per a temes de seguretat de la informació en els quals, entre d'altres, s'avaluen els resultats d'aquests mesuraments – veure els annexos 15. i 16. .
- ➔ El nivell de maduresa del requisit augmenta a 5, ja que es pressuposa un procés constant de mesurament, anàlisi i avaluació. Amb cada iteració, serà possible optimitzar una mica més els controls corresponents.

10.1.1: Hi ha un procediment documentat per identificar i registrar les no-conformitats i el seu tractament?

- ➔ Els indicadors són una eina fonamental per a la identificació i el registre de les no-conformitats.
- ➔ El nivell de maduresa del requisit augmenta a 4.

A més dels requisits esmentats de forma explícita, la realització del projecte d'implantació i gestió d'indicadors de seguretat possibilita la millora d'altres requisits, en tant en quan proporciona les eines per a que els nivells de maduresa passin a un nivell 4 (GESTIONAT I MESURABLE).

7.2.4 Millora del compliment dels controls ISO/IEC 27002

En quant als controls ISO/IEC 27002, i de forma anàloga a la millora del compliment de la norma ISO/IEC 27001 – veure 7.2.3 – l'impacte fonamental de l'aplicació del present projecte és que possibilita que els controls evolucionin fins al nivell 4 de maduresa (GESTIONAT I MESURABLE). Es tracta d'una millora transversal que afecta a tots els controls, en tant en quan es proporciona la base tècnica i organitzativa per a fer avançar els controls cap a un estat mesurable que, al seu torn, en possibilita la seva gestió. Aquesta

mesurabilitat i gestió, a més, també són un prerequisit per a fer evolucionar els controls cap a un nivell 5 (OPTIMITZAT). Aquest darrer pas no es contempla dins del present projecte.

La millora que proporciona el present projecte permet, doncs, cobrir una de les principals mancances de l'SGSI de l'Organització: la falta d'indicadors o manca de mesures clares i objectives de mesurament, tal i com s'observa a l'anàlisi de compliment inicial – veure 4.2 .

7.3 Projecte 3: Establiment de revisions periòdiques: de la direcció, auditories internes i auditories externes

El present projecte persegueix l'objectiu principal de millorar l'SGSI de l'Organització mitjançant la definició, planificació i execució de revisions periòdiques. Aquestes revisions pretenen proporcionar una visió actualitzada de l'estat dels sistemes de seguretat i detectar possibles punts de millora, ja sigui en l'àmbit de la seguretat de la informació o en altres àmbits de l'Organització. El projecte contempla l'establiment de diferents tipus de revisions:

- **Revisions per la direcció**: Es tracta de revisions generals de l'SGSI de l'Organització, gestionades i liderades per l'equip directiu de l'Organització. A l'annex 15. es troba definit el procediment establert per a aquestes reunions, així com els participants potencials (a més de la direcció), l'agenda a tractar i la periodicitat a seguir.

- **Auditories internes**: Les auditories són revisions periòdiques i exhaustives de l'SGSI de l'Organització. Al contrari que en el cas de les revisions per la direcció, les auditories internes estan clarament enfocades a avaluar el compliment de la norma ISO/IEC 27001 [3], a més de perseguir l'objectiu comú de millora del nivell de seguretat de l'Organització. En quant a la responsabilitat de l'organització i gestió de les auditories, aquesta recau en el CISO de l'Organització. A l'annex 13. es troba definit el procediment a seguir per a les auditories internes, incloent la programació temporal i el model d'informe a aplicar.

- **Auditories externes**: Aquest últim tipus de revisió es proposa com a extensió de les auditories internes. Les auditories externes són aquelles en les quals participen entitats externes a l'Organització (normalment consultors experts en ISO/IEC 27000), ja sigui amb la finalitat última d'aconseguir un certificat oficial de conformitat amb l'estàndard, o bé pel mer fet d'obtenir una visió externa. Aquest últim punt aporta un valor afegit a l'auditoria, en tant en quan s'eliminen possibles prejudicis previs a l'hora de dur a terme els anàlisis i les valoracions, ja que de forma externa es garanteix una visió no influenciada de la situació.

El present projecte contempla, doncs, la planificació i execució de les activitats necessàries per a dur a terme les revisions proposades.

7.3.1 Fases del projecte

Es consideren les següents fases en les quals es pot descompondre el present projecte.

Reunions inicials per definir les tasques i recursos necessaris:

Es tracta de reunions del grup de treball, en les quals s'analitza el procediment a seguir a l'hora de dur a terme les revisions, en base a l'establert als annexos 15. i 13. . A més, també s'assignaran els recursos necessaris per a la realització de les revisions, en funció de la periodicitat establerta i dels participants necessaris. Els recursos establerts en aquesta fase hauran d'incloure els diversos tipus de revisions que es duran a terme posteriorment: revisions per la direcció, auditories internes i auditories externes.

Els participants necessaris d'aquesta primera fase del projecte, juntament amb el conjunt d'hores estimades, es veuen recollits en la següent taula.

Personal	# hores internes	# hores externes
Directiu	16	
CISO	16	
IT Manager	8	

Taula 41: Cost estimat - projecte 3: definició de tasques i recursos

Del conjunt d'hores pressupostades a la taula 41, obtenim que la valoració econòmica de la present fase és de **1.000 €**.

Els objectius de les reunions i avaluacions inicials es poden programar amb un horitzó temporal de **curt termini**.

Realització de les revisions per la direcció:

En aquesta fase es contemplen les activitats relacionades amb la realització de les revisions periòdiques per la direcció. Cal comptabilitzar doncs, principalment, les activitats de preparació de les reunions, el temps empleat en les reunions pròpiament, i el temps necessari per a documentar els temes tractats en les mateixes.

Tal i com es defineix a l'annex 15. , es realitzarà, com a mínim, una revisió anual per part de la direcció de l'Organització. En cas necessari, es poden convocar 2 o més reunions en un any. En la següent taula es mostren els participants necessaris per aquesta fase, juntament amb el conjunt d'hores estimades, assumint una mitjana de 1,5 reunions anuals. Els recursos necessaris són un nou cost recurrent que tindrà l'Organització amb l'aplicació del present projecte.

Personal	# hores internes	# hores externes
Directiu	12	
CISO	10	
IT Manager	8	
Treballadors de RRHH	3	
Responsable de desenvolupament	3	
Responsable d'operacions	3	
Responsable de qualitat	3	

Taula 42: Cost estimat - projecte 3: revisions per la direcció

Del conjunt d'hores pressupostades a la taula 42, obtenim que la valoració econòmica de la present fase – recordem, de forma anual – és de **1.050 €**.

La planificació temporal de les revisions per la direcció es pot considerar a **mig i llarg termini**.

Realització d'auditories internes:

En aquesta fase es contemplen les activitats relacionades amb la realització d'auditories internes. Cal comptabilitzar doncs, principalment, les activitats de preparació de les auditories i l'execució de les mateixes.

Tal i com es defineix a l'annex 13. , la periodicitat màxima de realització d'auditories internes és de 12 mesos, podent-se reduir si el CISO o el Comitè de seguretat de la informació ho considera necessari. En la següent taula es mostren els participants necessaris per aquesta fase (mínim dues persones, segons l'establert als procediments; màxim no establert), juntament amb el conjunt d'hores estimades, assumint que es duu a terme una auditoria interna cada any. Els recursos necessaris són un nou cost recurrent que tindrà l'Organització amb l'aplicació del present projecte.

Personal	# hores internes	# hores externes
CISO	24	
IT Manager	24	
Treballadors de l'àrea de seguretat i/o de l'àrea d'IT	24	

Taula 43: Cost estimat - projecte 3: auditories internes

Del conjunt d'hores pressupostades a la taula 43, obtenim que la valoració econòmica de la present fase – recordem, de forma anual – és de **1.800 €**.

La planificació temporal de les auditories internes es pot considerar a **mig i llarg termini**.

Realització d'auditories externes:

En aquesta fase es contemplen les activitats relacionades amb la realització d'auditories externes. Cal comptabilitzar doncs, principalment, les activitats de preparació de les auditories i l'execució de les mateixes.

En el cas de les auditories externes es considera una periodicitat de 24 mesos (al contrari que per a les auditories internes, que és de 12 mesos). En quant al contingut i participants, les auditories externes són equiparables a les auditories internes, amb la diferència que s'afegeixen participants externs en les activitats.

En la següent taula es mostren els participants necessaris per aquesta fase, juntament amb el conjunt d'hores estimades, assumint que es duu a terme una auditoria externa cada 2 anys. A fi i efecte d'obtenir una visió clara i comparable amb els altres tipus de revisions, es calculen els recursos de forma anual. Es considera, per tant, la realització de 0,5 auditories externes a l'any. Els recursos necessaris són un nou cost recurrent que tindrà l'Organització amb l'aplicació del present projecte.

Personal	# hores internes	# hores externes
CISO	12	
IT Manager	12	
Treballadors de l'àrea de seguretat i/o de l'àrea d'IT	12	
Consultor extern 1: expert en ISO/IEC 27000		12
Consultor extern 2: expert en ISO/IEC 27000		12

Taula 44: Cost estimat - projecte 3: auditories externes

Del conjunt d'hores pressupostades a la taula 44, obtenim que la valoració econòmica de la present fase – recordem, de forma anual – és de **2.100 €**.

La planificació temporal de les auditories externes es pot considerar a **mig i llarg termini**.

7.3.2 Millora del risc

Els riscos associats als processos de negoci de l'Organització es veuen beneficiats de forma generalitzada degut a l'aplicació del present projecte i, de forma similar al cas del projecte descrit a 7.2 , degut a la naturalesa transversal del mateix.

Les diverses revisions periòdiques possibiliten el coneixement de l'estat actual de tots els requisits i controls establerts a l'SGSI i, al seu torn, afavoreixen la identificació d'oportunitats de millora. Aquestes avaluacions i millores porten a una reducció dels riscos identificats a 6. . Degut a la dificultat de quantificar el benefici que proporciona un projecte tan transversal, assumim una millora generalitzada del 10%, entenent-se com a una reducció de l'impacte potencial de les diferents amenaces.

7.3.3 Millora del compliment de la norma ISO/IEC 27001

Els requisits de la norma ISO/IEC 27001 que es veurien millorats per l'aplicació del present projecte són:

4.4.1: El sistema de Gestió de Seguretat de la informació SGSI està establert, implementat i es revisa de manera planificada considerant oportunitats de millora?

- ➔ El SGSI està establert a l'Organització. Un cop s'apliqui el present projecte, a més, aquest es revisa de manera planificada, tant temporalment com en quant al contingut de les revisions.

➔ El nivell de maduresa del requisit augmenta a 5, considerant que les revisions es duen a terme durant diverses iteracions.

5.1.2: La direcció proveeix dels recursos materials i humans necessaris per al compliment dels objectius del SGSI?

➔ Les revisions periòdiques, en especial les revisions per la direcció, afavoreixen l'assignació dels recursos necessaris per al compliment dels objectius del SGSI.
➔ El nivell de maduresa del requisit augmenta a 4.

5.1.3: La direcció revisa directament l'eficàcia de l'SGSI per garantir que es compleixen els objectius de l'SGSI?

➔ Un dels tipus de revisions periòdiques són les revisions (directament) per la direcció.
➔ El nivell de maduresa del requisit augmenta a 4.

7.1.1: S'identifiquen i assignen els recursos necessaris per a l'SGSI?

➔ De forma similar al requisit 5.1.2, les revisions per la direcció possibiliten que s'assignin els recursos necessaris per a l'SGSI.
➔ El nivell de maduresa del requisit augmenta a 4.

9.1.2: S'ha establert un procés documentat per avaluar els resultats dels mesuraments i que aquests resultats són presos en compte pels responsables tant dels processos com de la Seguretat de la informació?

➔ De forma similar al què s'exposa a 7.2.3 , el present projecte també millora la manera d'avaluar els resultats, per part dels rols corresponents a l'Organització.
➔ El nivell de maduresa del requisit augmenta a 5.

9.2.1: S'ha establert una programació d'auditories internes i assignat responsables?

➔ Un dels tipus de revisions periòdiques són les auditories internes.
➔ El nivell de maduresa del requisit augmenta a 4.

9.2.2: L'abast i els requisits s'han definit per a l'informe d'auditoria?

➔ El contingut, abast i requisits de l'informe d'auditoria està definit a l'annex 13. . L'aplicació del present projecte, a més, possibilita la planificació i execució de les auditories.
➔ El nivell de maduresa del requisit augmenta a 4.

9.2.3: Es consideren accions correctives i propostes de canvi als informes d'auditoria?

➔ Un dels elements continguts als informes d'auditoria són les recomanacions de millora.
➔ El nivell de maduresa del requisit augmenta a 4.

9.3.1: Hi ha una programació per als informes de la direcció i hi ha constància de la seva realització periòdica?

- ➔ Les revisions periòdiques per la direcció, tal i com estan definides a l'annex 15. , descriuen els punts a tractar com a part de l'agenda de la revisió. Aquesta, a més, també considera l'estat de les revisions anteriors.
- ➔ El nivell de maduresa del requisit augmenta a 4.

9.3.2: Es documenten els resultats dels informes i la direcció s'implica tant en el coneixement com en la presa de decisions sobre els aspectes crucials per al SGSI?

- ➔ Les revisions periòdiques per la direcció especifiquen com s'han de documentar els punts tractats a cada reunió (en forma de MoM o *Minutes of Meeting*).
- ➔ El nivell de maduresa del requisit augmenta a 4.

10.1.1: Hi ha un procediment documentat per identificar i registrar les no-conformitats i el seu tractament?

- ➔ Un dels elements continguts als informes d'auditoria són les no-conformitats detectades, a més de les possibles recomanacions de millora.
- ➔ El nivell de maduresa del requisit augmenta a 4.

10.2.1: Hi ha un procés per garantir la millora contínua de l'SGSI identificant les oportunitats de millora?

- ➔ Els diferents revisions proposades pel present projecte afavoreixen la possibilitat de millora contínua de l'SGSI de l'Organització. Aquest requisit podria, amb el temps, evolucionar fins a un nivell de maduresa 5.
- ➔ El nivell de maduresa del requisit augmenta, per ara, al nivell 4.

A més dels requisits esmentats de forma explícita, la realització del projecte, especialment en les revisions de tipus auditories, influeix positivament en tota la resta de requisits de la norma ISO/IEC 27001, en tant en quan la revisió dels mateixos afavoreix la detecció de possibles punts de millora. Les revisions periòdiques són, a més, un requisit indispensable per a fer evolucionar els nivell de maduresa dels requisits de 4 (GESTIONAT I MESURABLE) a 5 (OPTIMITZAT).

7.3.4 Millora del compliment dels controls ISO/IEC 27002

Els controls ISO/IEC 27002 que es veurien millorats per l'aplicació del present projecte són:

A.5.1.2: Revisió de les polítiques per la seguretat de la informació

- ➔ Un dels objectius de les revisions periòdiques és avaluar la conformitat i actualitat de les polítiques per la seguretat de la informació.
- ➔ El nivell de maduresa del control augmenta a 4.

A.9.2.5: Revisió dels drets d'accés d'usuari

- ➔ Les revisions periòdiques possibiliten avaluar si els drets d'usuari segueixen essent vàlids o si, pel contrari, requereixen d'una actualització.

➔ El nivell de maduresa del control augmenta a 4.

A.12.7.1: Controls d'auditoria de sistemes d'informació

➔ Un dels tipus de revisions periòdiques són les auditories internes.
➔ El nivell de maduresa del control augmenta a 4.

A.15.2.1: Control i revisió de la provisió de serveis del proveïdor

➔ Realitzar revisions periòdiques afavoreix el control i avaluació del servei prestat pels proveïdors de serveis.
➔ El nivell de maduresa del control augmenta a 4.

A.16.1.4: Avaluació i decisió sobre els events de seguretat de la informació

➔ Les revisions periòdiques, concretament les revisions per la direcció, permeten avaluar i prendre decisions sobre incidents de seguretat succeïts.
➔ El nivell de maduresa del control augmenta a 4.

A.16.1.6: Aprenentatge dels incidents de seguretat de la informació

➔ Com a conseqüència de les avaluacions dels incidents – control A.16.1.4 – i en el marge de les revisions periòdiques, és ara possible aprendre dels incidents i prendre mesures per a millorar l'estat general de l'SGSI.
➔ El nivell de maduresa del control augmenta a 5, entenent que es duen a terme varies iteracions de revisions i, per tant, de millores apreses (el que en anglès s'anomena *lessons learnt*).

A.17.1.3: Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació

➔ Les revisions periòdiques afavoreixen la verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.
➔ El nivell de maduresa del control augmenta a 4.

A.18.2.1: Revisió independent de la seguretat de la informació

➔ Les revisions periòdiques, concretament les auditories (en especial les externes), permeten una revisió independent de l'SGSI.
➔ El nivell de maduresa del control augmenta a 4.

A.18.2.2: Compliment de les polítiques i normes de seguretat

➔ Les revisions tenen com a objectiu avaluar el compliment de les polítiques i normes de seguretat en l'àmbit de seguretat de l'Organització.
➔ El nivell de maduresa del control augmenta a 4.

A.18.2.3: Comprovació del compliment tècnic

➔ Les revisions tenen com a objectiu avaluar el compliment tècnic en l'àmbit de seguretat de l'Organització.
➔ El nivell de maduresa del control augmenta a 4.

A més dels controls esmentats de forma explícita, i de forma similar a com s'exposa a 7.3.3 , la realització del projecte millora de forma transversal tots els controls ISO/IEC 27002, en tant en quan la revisió dels mateixos en possibilita el coneixement de l'estat actual i n'afavoreix la detecció de possibles punts de millora.

7.4 Projecte 4: Adopció de *Security by Design* als processos de l'Organització

El present projecte, a més d'abordar aspectes organitzatius de l'SGSI i contràriament als altres projectes proposats, també te un enfocament marcadament tècnic. L'objectiu principal del projecte és el d'adoptar el concepte de *Security by Design* (o seguretat des del disseny) en els processos de negoci de l'Organització. De forma sintetitzada, aquest concepte es refereix al fet de considerar la seguretat dels sistemes des de les fases inicials d'un procés o d'un producte. És a dir, des del disseny. En el cas de l'SGSI, s'entén com a producte tots aquells sistemes que formen part dels actius de l'Organització – veure inventari d'actius a 6. . Tot i incloure el disseny de qualsevol dels actius, el concepte de *Security by Design* fa especial referència a la concepció de noves aplicacions, elements de xarxa, serveis i equipament de hardware.

El present projecte contempla, doncs, les activitats necessàries per a implementar el concepte de seguretat des del disseny, tant en els processos com en els nous productes de l'Organització.

7.4.1 Fases del projecte

Es consideren les següents fases en les quals es pot descompondre el present projecte.

Reunions inicials per definir les tasques i recursos necessaris:

Es tracta de reunions del grup de treball, els objectius principals de les quals són, primerament, analitzar quin és l'estat actual de l'adopció de *Security by Design* en els diferents processos de l'Organització i en la creació de nous productes i, posteriorment, decidir quines tasques es duran a terme i amb quins recursos per a incrementar el nivell de seguretat des del disseny.

Els participants necessaris d'aquesta primera fase del projecte, juntament amb el conjunt d'hores estimades, es veuen recollits en la següent taula. Es pot destacar que, tot i el caràcter principalment tècnic del present projecte, en aquesta fase també es necessària la participació

de la direcció de l'Organització, ja que un dels objectius és la presa de decisions sobre els recursos a assignar a les diferents tasques.

Personal	# hores internes	# hores externes
Directiu	4	
CISO	8	
IT Manager	8	
Responsable de desenvolupament	8	
Responsable d'operacions	8	
Responsable de qualitat	4	

Taula 45: Cost estimat - projecte 4: definició de tasques i recursos

Del conjunt d'hores pressupostades a la taula 45, obtenim que la valoració econòmica de la present fase és de **1.000 €**.

Els objectius de les reunions i avaluacions inicials es poden programar amb un horitzó temporal de **curt termini**.

Implementació de les mesures definides per a millorar la seguretat en el disseny:

En aquesta fase es duu a terme la implementació de totes aquelles mesures acordades en la fase anterior. Les activitats que conformen el conjunt de mesures a aplicar poden ser de caire molt variat. A continuació es mostren alguns exemples de les mateixes:

- Prèviament a l'inici del desenvolupament d'un producte o de la posada en marxa d'un nou procès, avaluar les competències en seguretat de tot el personal implicat i considerar-ne la seva idoneïtat. Aquesta avaluació i decisió també aplica a proveïdors de serveix i altres subcontractistes.

- Realitzar un anàlisi i avaluació, des del punt de vista de la seguretat de la informació, abans de realitzar cap canvi en els sistemes. És a dir, no només avaluar els canvis des del punt de vista funcional.

- Possibilitar (o millorar) la separació dels recursos en els diferents entorns: desenvolupament, prova o validació, i operació. Relacionat amb aquest aspecte, millorar la separació física i lògica entre els diferents entorns.

- Adoptar criteris de seguretat de la informació a l'hora de plantejar el disseny de nous desenvolupaments (concretament de software) que, per exemple, afavoreixin o descartin certes tecnologies.

En la següent taula es mostren els participants necessaris per aquesta fase, juntament amb el conjunt d'hores estimades. Les tasques pertanyents a aquesta fase són activitats recurrents. Així doncs, el càlcul de recursos fa referència a les hores anuals necessàries que, en conseqüència, caldrà adoptar com a nou cost recurrent un cop s'hagi aprovat la implantació del projecte.

Personal	# hores internes	# hores externes
CISO	8	
Treballadors de l'àrea de seguretat	16	
IT Manager	8	
Treballadors de l'àrea d'IT	24	
Responsable de desenvolupament	8	
Treballadors de l'àrea de desenvolupament	40	
Responsable d'operacions	8	
Treballadors de l'àrea d'operacions	32	
Responsable de qualitat	8	
Treballadors de l'àrea de qualitat	16	
Proveïdors de serveis		16
Altres tercers		16

Taula 46: Cost estimat - projecte 4: implantació de mesures

Del conjunt d'hores pressupostades a la taula 46, obtenim que la valoració econòmica de la present fase – recordem, de forma anual – és de **5.800 €**.

La planificació temporal de les activitats d'aquesta fase es pot considerar a **mig i llarg termini**.

7.4.2 Millora del risc

Els riscos associats als processos de negoci de l'Organització, en el cas d'aplicació del present projecte, es veurien afectats de la següent forma:

Averia de l'equipament o programa (físic o lògic)

- ➔ El fet de considerar aspectes de seguretat en el disseny dels productes (sobretot en el cas dels programes), redueix la probabilitat que hi hagi una averia en els mateixos.
- ➔ La vulnerabilitat o freqüència es redueix a 1/10.

Incident en la xarxa de comunicacions

- ➔ Dissenyar les xarxes de comunicacions tenint en compte criteris de seguretat de la informació influeix positivament en la mitigació d'aquest risc. És força improbable, però, reduir-ne la freqüència d'ocurrència (totes les xarxes pateixen incidents). L'aplicació del present projecte, en canvi, pot ajudar a reduir l'impacte que la consecució de l'amenaça tindria sobre l'SGSI de l'Organització.
- ➔ L'impacte potencial es veu reduït en un 20%.

Error d'ús dels sistemes

- ➔ L'aplicació de mesures de seguretat en el disseny dels sistemes afavoreix la reducció d'errors a l'hora de fer-ne ús, ja que s'impossibilita que certes accions desencadenin en fallades del sistema.
- ➔ La vulnerabilitat o freqüència es redueix a 1.

Error d'administració dels sistemes

- ➔ De forma similar al cas d'ús dels sistemes, l'adopció de mesures de *Security by Design* aconsegueixen l'objectiu de reduir els errors d'administració de sistemes.
- ➔ La vulnerabilitat o freqüència es redueix a 1.

Incidents deguts a software malintencionat

- ➔ Un disseny segur permet reduir l'impacte que els incidents degut a software malintencionat tindrien en l'SGSI de l'Organització. A més, també és presumible que la probabilitat de materialització de l'amenaça minvi.
- ➔ L'impacte potencial es veu reduït en un 20%. A més, la vulnerabilitat o freqüència es redueix a 1/10.

Alteració de la informació

- ➔ L'adopció de *Security by Design* possibilita la reducció d'events d'alteració de la informació. A més, l'impacte en cas d'incident es veu disminuït (les mesures de seguretat fan que no s'afecti a la totalitat del sistema).
- ➔ La vulnerabilitat o freqüència es redueix a 1/10, i l'impacte potencial en un percentatge del 20%.

Destrucció de la informació

- ➔ De forma similar al risc d'alteració de la informació, el projecte també redueix en la mateixa mesura el risc de destrucció de la informació.
- ➔ La vulnerabilitat o freqüència es redueix a 1/10, i l'impacte potencial en un percentatge del 20%.

Fuga d'informació

- ➔ De forma similar al risc d'alteració de la informació, el projecte també redueix en la mateixa mesura el risc de fuga d'informació.
- ➔ La vulnerabilitat o freqüència es redueix a 1/10, i l'impacte potencial en un percentatge del 20%.

Intercepció d'informació

- ➔ De forma similar al risc d'alteració de la informació, el projecte també redueix en la mateixa mesura el risc d'intercepció d'informació.
- ➔ La vulnerabilitat o freqüència es redueix a 1/10, i l'impacte potencial en un percentatge del 20%.

7.4.3 Millora del compliment de la norma ISO/IEC 27001

Els requisits de la norma ISO/IEC 27001 que es veurien millorats per l'aplicació del present projecte són:

6.2.3: S'han integrat els objectius de la Seguretat de la Informació als processos de l'organització tenint en compte les funcions principals dins de l'Organització?

- ➔ La consideració i aplicació d'elements de seguretat des del disseny dels processos i productes possibilita que s'integrin els objectius de seguretat definits a les polítiques.
- ➔ El nivell de maduresa del requisit augmenta a 4.

7.2.1: S'avalua la competència en matèries de seguretat de la informació per a persones que efectuen tasques que puguin afectar la seguretat?

- ➔ Decidir l'assignació de tasques a persones en funció de la seva competència en matèries de seguretat constitueix una possible activitat de seguretat des del disseny (de processos).
- ➔ El nivell de maduresa del requisit augmenta a 4.

8.1.2: Hi ha un procés per avaluar els riscos a la Seguretat de la Informació abans de realitzar canvis en el Sistema de Gestió o processos de Seguretat?

- ➔ Avaluar els riscos abans de realitzar canvis que puguin afectar a la seguretat de la informació és una possible activitat de seguretat des del disseny (de processos i d'actius).
- ➔ El nivell de maduresa del requisit augmenta a 4.

8.1.4: S'identifiquen i es controlen els processos externalitzats quant als riscos per a la Seguretat de la Informació?

- ➔ De forma similar al requisit 8.1.2, també és d'aplicació per al projecte una avaluació de riscos en el cas d'adopció dels processos externalitzats.
- ➔ El nivell de maduresa del requisit augmenta a 4.

7.4.4 Millora del compliment dels controls ISO/IEC 27002

Els controls ISO/IEC 27002 que es veurien millorats per l'aplicació del present projecte són:

A.6.1.5: Seguretat de la informació en la gestió de projectes

- ➔ Es tenen en compte aspectes de seguretat de la informació en totes les fases de gestió dels projectes, incloent les fases inicials.
- ➔ El nivell de maduresa del control augmenta a 4.

A.12.1.4: Separació dels recursos de desenvolupament, prova i operació

- ➔ Separar els diferents entorns existents en les xarxes i sistemes de l'Organització és una bona mesura en termes de seguretat de la informació.
- ➔ El nivell de maduresa del control augmenta a 4.

A.12.5.1: Instal·lació del software en explotació

- ➔ El software s'avalua exhaustivament abans de passar a entorns productius. Aquesta avaluació, a més de seguir criteris funcionals, també tindria en compte aspectes de seguretat de la informació.
- ➔ El nivell de maduresa del control augmenta a 4.

A.13.1.2: Seguretat dels serveis de xarxa

- ➔ Els aspectes de seguretat en el disseny també es tenen en compte en els serveis de xarxa.
- ➔ El nivell de maduresa del control augmenta a 4.

A.13.1.3: Segregació en xarxes

- ➔ De forma similar a la separació d'entorns – control A.12.1.4 –, la segregació de xarxes també millora la seguretat de l'SGSI.
- ➔ El nivell de maduresa del control augmenta a 4.

A.14.1.1: Anàlisi de requisits i especificacions de seguretat de la informació

- ➔ A l'hora de desenvolupar nous sistemes (e.g. noves aplicacions), es duria a terme un anàlisi de requisits de seguretat, ja des de fases inicials del procés de desenvolupament.
- ➔ El nivell de maduresa del control augmenta a 4.

A.14.1.3: Protecció de les transaccions de serveis d'aplicacions

- ➔ Es millora el nivell de seguretat de les transaccions de dades entre aplicacions.
- ➔ El nivell de maduresa del control augmenta a 4.

A.14.2.1: Política de desenvolupament segur

- ➔ Implementar la política de desenvolupament segur, referenciada a l'annex 12. , és un mecanisme imprescindible per a garantir la consideració d'aspectes de seguretat en el desenvolupament de nou software.

➔ El nivell de maduresa del control augmenta a 4.

A.14.2.5: Principis d'enginyeria de sistemes segurs

➔ De forma similar al control A.14.2.1, en aquest cas es milloraria la seguretat en l'enginyeria de sistemes i processos.
➔ El nivell de maduresa del control augmenta a 4.

A.14.2.6: Entorn de desenvolupament segur

➔ L'entorn on es desenvolupa nou software – el qual, pel mer fet d'estar sota desenvolupament, no pot considerar-se encara segur – no te ni pot tenir cap afectació a altres entorns de l'Organització.
➔ El nivell de maduresa del control augmenta a 4.

A.14.2.8: Proves funcionals de seguretat de sistemes

➔ Els nous sistemes (o canvis en els existents) s'han de provar tenint en compte varies dimensions de funcionalitat: que compleixin amb els objectius pels quals han estat dissenyats i, a més, que compleixin amb els requisits de seguretat establerts.
➔ El nivell de maduresa del control augmenta a 4.

A.14.2.9: Proves d'acceptació de sistemes

➔ Els nous sistemes (o canvis en els existents) es validarien abans de passar a entorns de producció. Aquestes proves, a més de ser funcionals, també han de seguir criteris de seguretat de la informació.
➔ El nivell de maduresa del control augmenta a 4.

7.5 Millores intrínseques (MI) per la realització del pla director de seguretat de l'Organització

Independentment de la realització (o no) dels diferents projectes proposats, l'elaboració del pla director de seguretat – és a dir, la redacció del present treball de màster aplicat a la realitat de l'Organització – ja constitueix una millora en diferents aspectes de l'SGSI de l'Organització. Als capítols 7.5.1 , 7.5.2 i 7.5.3 es descriu quina és l'evolució dels diferents apartats.

A l'hora d'assolir les millores descrites a continuació no es pressuposa cap cost afegit. Si es volgués definir, a posteriori, els recursos necessaris, caldria comptabilitzar totes les hores invertides per a l'elaboració i redacció del present pla director de seguretat.

7.5.1 Millora del risc

La realització del pla director de seguretat de l'Organització contribueix a possibilitar un anàlisi del risc intrínsec als processos de negoci existents. Aquest anàlisi, al seu torn, és imprescindible per a gestionar el risc de manera controlada. És de particular rellevància l'anàlisi de riscos realitzat – veure 6. .

Tot i definir les bases per a la realització d'anàlisis de riscos, el pla director de seguretat, per si mateix, no redueix els riscos de l'Organització.

7.5.2 Millora del compliment de la norma ISO/IEC 27001

Els requisits de la norma ISO/IEC 27001 que es veuen millorats per l'elaboració del present pla director de seguretat són:

4.1.1: Estan identificats els objectius del SGS Sistema de Gestió de la Seguretat de la Informació?

- ➔ Els objectius estan identificats i ara, a més, es poden mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del requisit augmenta a 4.

4.1.2: S'han identificat les qüestions internes i externes relacionades amb la seguretat de la informació?

- ➔ De forma similar al requisit 4.1.1, les qüestions internes i externes ara es poden mesurar.
- ➔ El nivell de maduresa del requisit augmenta a 4.

4.1.3: S'han identificat com les parts internes i externes poden suposar amenaces o riscos per a la seguretat de la informació?

- ➔ L'anàlisi de riscos realitzat – veure 6. – considera amenaces internes i externes.
- ➔ El nivell de maduresa del requisit augmenta a 3.

4.2.1: S'han identificat les parts interessades?

- ➔ Les parts interessades estan identificades a la política de seguretat de la informació.
- ➔ El nivell de maduresa del requisit augmenta a 3.

4.2.2: Hi ha un llistat de requisits sobre Seguretat de la Informació de les parts interessades?

- ➔ Els requisits estan llistats a la política de seguretat de la informació.
- ➔ El nivell de maduresa del requisit augmenta a 4.

4.2.3: Hi ha un llistat de requisits sobre Seguretat de la Informació referent a reglaments, requisits legals i requisits contractuals?

- ➔ Els requisits legals i contractuals queden recollits a la política de seguretat de la informació.

➔ El nivell de maduresa del requisit augmenta a 4.

4.3.1: S'ha determinat l'abast del SGS i se'n conserva informació documentada?

➔ L'abast del SGSI està definit en el present pla director de seguretat de l'Organització.
➔ El nivell de maduresa del requisit augmenta a 3.

5.1.1: S'han establert objectius de la Seguretat de la Informació d'acord amb els objectius del negoci?

➔ Els objectius de la seguretat de la informació estan definits, de forma alineada amb els objectius de negoci de l'Organització, a la política de seguretat de la informació.
➔ El nivell de maduresa del requisit augmenta a 4.

5.2.1: S'ha definit una política de seguretat de la informació?

➔ La política es pot trobar definida a l'annex 12. .
➔ El nivell de maduresa del requisit augmenta a 4.

5.2.4: Es manté informació documentada de la política de l'SGSI i dels seus objectius?

➔ La política es pot trobar definida a l'annex 12. .
➔ El nivell de maduresa del requisit augmenta a 4.

5.3.1: S'han assignat les responsabilitats i les autoritats sobre la Seguretat de la Informació?

➔ Els rols i responsabilitats es troben definits a l'annex 16. .
➔ El nivell de maduresa del requisit augmenta a 4.

6.1.2: S'identifiquen i analitzen els riscos mitjançant un mètode d'avaluació i d'acceptació de riscos?

➔ Es duu a terme un anàlisi de riscos basat en la metodologia Magerit – veure annex 17. .
➔ El nivell de maduresa del requisit augmenta a 4.

6.1.4: S'han establert criteris per elaborar una declaració d'aplicabilitat?

➔ La declaració d'aplicabilitat dels controls ISO/IEC 27002 a l'SGSI de l'Organització es pot trobar definida l'annex 18. .
➔ El nivell de maduresa del requisit augmenta a 4.

6.1.5: Es manté informació documentada dels punts anteriors?

➔ Existeix documentació tant per al control 6.1.2 (metodologia d'anàlisi de riscos) com per al control 6.1.4 (declaració d'aplicabilitat).
➔ El nivell de maduresa del requisit augmenta a 4.

6.2.1: S'han establert objectius de la Seguretat de la Informació mesurables i d'acord amb els objectius del negoci?

➔ Els objectius de la seguretat de la informació estan definits, de forma alineada amb els objectius de negoci de l'Organització, a la política de seguretat de la informació.

➔ El nivell de maduresa del requisit augmenta a 4.

7.5.1: Es disposa de la documentació requerida per la norma més la requerida per l'organització incloent-hi? (veure la norma ISO/IEC 27001 [3] per al requisit sencer)

➔ La documentació requerida es troba definida en el present pla director de seguretat de l'Organització.
➔ El nivell de maduresa del requisit augmenta a 4.

8.2.1: S'ha establert un procés documentat d'anàlisi i d'avaluació de riscos per a la seguretat de la informació on s'identifiqui? (veure la norma ISO/IEC 27001 [3] per al requisit sencer)

➔ S'ha documentat tant la metodologia per a realitzar un anàlisi de riscos – veure annex 17. – com l'anàlisi de riscos efectuat sobre els actius de l'Organització – veure 6. .
➔ El nivell de maduresa del requisit augmenta a 4.

8.3.2: S'identifiquen tots els controls necessaris per mitigar el risc justificant-ne l'aplicació?

➔ Els controls aplicables a l'SGSI estan definits en la declaració d'aplicabilitat.
➔ El nivell de maduresa del requisit augmenta a 3.

8.3.3: Es documenta el nivell d'aplicació de tots els controls que cal aplicar?

➔ Els controls aplicables (i els no aplicables) a l'SGSI estan definits en la declaració d'aplicabilitat.
➔ El nivell de maduresa del requisit augmenta a 3.

9.1.1: S'ha establert un procés continu de monitorització dels aspectes clau de la seguretat de la informació tenint en compte els controls per a la seguretat de la informació?

➔ Les diferents revisions i els indicadors de seguretat possibiliten la monitorització.
➔ El nivell de maduresa del requisit augmenta a 4.

9.1.2: S'ha establert un procés documentat per avaluar els resultats dels mesuraments i que aquests resultats són presos en compte pels responsables tant dels processos com de la Seguretat de la informació?

➔ Les diferents revisions possibiliten l'avaluació dels resultats dels mesuraments.
➔ El nivell de maduresa del requisit augmenta a 5.

9.2.1: S'ha establert una programació d'auditories internes i assignat responsables?

➔ El procediment d'auditories internes es troba documentat a l'annex 13. .
➔ El nivell de maduresa del requisit augmenta a 4.

9.2.2: L'abast i els requisits s'han definit per a l'informe d'auditoria?

➔ El procediment d'auditories internes es troba documentat a l'annex 13. .
➔ El nivell de maduresa del requisit augmenta a 4.

9.2.3: Es consideren accions correctives i propostes de canvi als informes d'auditoria?

- ➔ Els informes d'auditoria consideren accions correctives i propostes de canvi.
- ➔ El nivell de maduresa del requisit augmenta a 4.

9.3.1: Hi ha una programació per als informes de la direcció i hi ha constància de la seva realització periòdica?

- ➔ El procediment de revisions periòdiques per la direcció es troba documentat a l'annex 15. .
- ➔ El nivell de maduresa del requisit augmenta a 4.

10.1.1: Hi ha un procediment documentat per identificar i registrar les no-conformitats i el seu tractament?

- ➔ Un dels elements continguts als informes d'auditoria són les no-conformitats detectades, a més de les possibles recomanacions de millora.
- ➔ El nivell de maduresa del requisit augmenta a 4.

10.2.1: Hi ha un procés per garantir la millora contínua de l'SGSI identificant les oportunitats de millora?

- ➔ Els diferents revisions proposades pel present projecte afavoreixen la possibilitat de millora contínua de l'SGSI de l'Organització. Aquest requisit podria, amb el temps, evolucionar fins a un nivell de maduresa 5.
- ➔ El nivell de maduresa del requisit augmenta, per ara, al nivell 4.

7.5.3 Millora del compliment dels controls ISO/IEC 27002

Els controls ISO/IEC 27002 que es veurien millorats per l'elaboració del present pla director de seguretat es llisten a continuació. Cal destacar que no tots els controls evolucionen a un nivell 4 (GESTIONAT I MESURABLE); només ho fan aquells que, o bé ja partien d'un nivell 3 (DEFINIT) i ara són mesurables (gràcies als indicadors de seguretat definits), o bé s'han definit durant el procés de redacció del pla director de seguretat.

A.5.1.2: Revisió de les polítiques per la seguretat de la informació

- ➔ Es defineixen els períodes de revisió de les polítiques.
- ➔ El nivell de maduresa del control augmenta a 4.

A.8.1.2: Propietat dels actius

- ➔ En l'anàlisi de riscos realitzat – veure 6. – es troba documentada la propietat de tots els actius.
- ➔ El nivell de maduresa del control augmenta a 4.

A.9.1.1: Política de control d'accés

- ➔ A més d'estar definida, ara, la política es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

A.9.1.2: Accés a les xarxes i als servidors de xarxa

- ➔ A la política de seguretat es referencia el reglament corresponent. Aquest, a més, es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

A.10.1.1: Política d'usos dels controls criptogràfics

- ➔ La política s'ha definit – veure annex 12. – i, a més, ara es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

A.10.1.2: Gestió de claus

- ➔ La política s'ha definit – veure annex 12. – i, a més, ara es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

A.11.2.6: Seguretat dels equips fora de les instal·lacions

- ➔ La política s'ha definit – veure annex 12. – i, a més, ara es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

A.13.2.1: Polítiques i procediments d'intercanvi d'informació

- ➔ La política s'ha definit – veure annex 12. – i, a més, ara es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

A.13.2.2: Acords d'intercanvi d'informació

- ➔ La política s'ha definit – veure annex 12. – i, a més, ara es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

A.13.2.3: Missatgeria electrònica

- ➔ La política s'ha definit – veure annex 12. – i, a més, ara es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

A.13.2.4: Acords de confidencialitat o no revelació

- ➔ La política s'ha definit – veure annex 12. – i, a més, ara es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

A.18.1.1: Identificació de la legislació aplicable i dels requisits contractuals

- ➔ La legislació aplicable i els requisits contractuals estan definits en la política de seguretat de la informació (com a «Marc regulador»).
- ➔ El nivell de maduresa del control augmenta a 4.

A.18.1.2: Drets de propietat intel·lectual (DPI)

- ➔ De forma similar al control A.18.1.1, a la política de seguretat de la informació (concretament, a «Marc regulador») es fa referència a les lleis de DPI que apliquen.
- ➔ El nivell de maduresa del control augmenta a 4.

A.18.1.5: Regulació dels controls criptogràfics

- ➔ S'ha definit la política corresponent – veure annex 12. – i, a més, ara es pot mesurar gràcies als indicadors de seguretat definits.
- ➔ El nivell de maduresa del control augmenta a 4.

Controls A.5.1.1, A.6.1.1, A.6.1.2, A.6.2.1, A.6.2.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.1.1, A.8.2.1, A.9.2.1, A.9.2.2, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3, A.9.4.4, A.11.1.1, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.4, A.12.1.3, A.12.1.4, A.12.3.1, A.12.4.4, A.13.1.1, A.14.1.2, A.15.1.1, A.16.1.1, A.17.1.2, A.17.2.1, A.18.1.4

- ➔ Aquests controls ja partien d'un nivell 3 (DEFINIT), i evolucionen ara a un nivell 4 (GESTIONAT I MESURABLE) gràcies als indicadors de seguretat definits.

7.6 Reducció dels riscos de l'Organització després dels projectes

En la següent taula es mostra quina seria l'evolució dels riscos associats als processos de negoci de l'Organització si apliquéssim els projectes proposats en els apartats 7.1 , 7.2 , 7.3 i 7.4 . Tal i com s'indica a 7.5.1 , no hi ha millores intrínseques (MI) en els riscos pel sol fet d'haver redactat el pla director de seguretat de l'Organització. D'altra banda, cal destacar que s'ha omès el propietari del risc, ja que aquest no varia en cap cas.

Amenaça	Impacte potencial	Vulnerabilitat o freqüència	Risc	Projectes que el redueixen
Incendi, per causes naturals o industrials	325.6*	1/10	32.56*	2, 3
Inundacions, per causes naturals o industrials	325.6*	1/10	32.56*	2, 3
Averia de l'equipament o programa (físic o lògic)	391.4*	1/10*	39.14*	2, 3, 4
Tall del subministre elèctric	219.2*	1	219.2*	2, 3
Averia en el sistema de climatització	178.6*	1	178.6*	2, 3
Incident en la xarxa de comunicacions	174.96*	10	1749.6*	2, 3, 4
Error d'ús dels sistemes	291.1*	1*	291.1*	1, 2, 3, 4
Error d'administració dels sistemes	774.5*	1*	774.5*	1, 2, 3, 4

Amenaça	Impacte potencial	Vulnerabilitat o freqüència	Risc	Projectes que el redueixen
Incidents deguts a software malintencionat	417.6*	1/10*	41.76*	1, 2, 3, 4
Alteració de la informació	122.16*	1/10*	12.22*	1, 2, 3, 4
Destrucció de la informació	147*	1/10*	14.7*	1, 2, 3, 4
Fuga d'informació	189.84*	1/10*	18.98*	1, 2, 3, 4
Error de manteniment / actualització de software	235.2*	1	235.2*	2, 3
Error de manteniment / actualització de hardware	214.4*	1/10	21.44*	2, 3
Accés no autoritzat	284.6*	1	284.6*	2, 3
Intercepció d'informació	156.72*	1/10*	15.67*	1, 2, 3, 4

Taula 47: Evolució del risc de les amenaces després dels projectes

*: el valor s'ha vist reduït gràcies a la implementació dels projectes proposats.

Tal i com es desprèn de la taula 47, tots els riscos de l'Organització es veuen reduïts en la dimensió de l'impacte potencial. A més a més, moltes de les probabilitats d'ocurrència de les amenaces també disminueixen, afavorint el reduir encara més el valor dels riscos residuals. La freqüència o probabilitat d'ocurrència és el principal factor determinant de la variació del risc (pels seus valors amb diferències múltiples de 10), tal i com s'exposa a l'anàlisi de riscos de l'Organització – veure 6. .

Les millores més destacables són les dels riscos relacionats amb errors d'ús o d'administració dels sistemes i, en menor mesura, totes aquelles amenaces la freqüència de les quals es veu reduïda. D'altra banda, el risc associat a incidents en la xarxa de comunicacions roman en valors elevats: tot i reduir-se en gran mesura el seu impacte potencial, els projectes proposats no aconsegueixen reduir-ne la probabilitat d'ocurrència.

A continuació es mostren, de forma molt resumida i per a facilitar un anàlisi ràpid, les millores del risc com a conseqüència de l'aplicació de cadascun dels projectes proposats. Per a més detall, veure el capítol corresponent: 7.1.2 , 7.2.2 , 7.3.2 , 7.4.2 o 7.5.1 .

- **Projecte 1 (campanyes)**: reducció de la vulnerabilitat o freqüència d'alguns riscos.
- **Projecte 2 (indicadors)**: reducció de l'impacte – en un 10% – de tots els riscos.
- **Projecte 3 (revisions)**: reducció de l'impacte – en un 10% – de tots els riscos.
- **Projecte 4 (*Security by Design*)**: reducció de la vulnerabilitat o freqüència d'alguns riscos, i de l'impacte – en un 20% – d'un subconjunt d'aquests riscos.

- **Millores intrínseques**: no hi ha una millora del risc.

7.7 Evolució del compliment de la norma ISO/IEC 27001 després dels projectes

En la següent taula es mostra quina seria l'evolució del compliment dels requisits definits en la norma ISO/IEC 27001, per part de l'Organització, si apliquéssim els projectes proposats en els apartats 7.1 , 7.2 , 7.3 i 7.4 , alhora que considerant les millores intrínseques (MI) per l'elaboració del pla director de seguretat 7.5 .

Requisits	Nivell de maduresa	Projectes que el milloren
4: L'Organització i el Context	**3.83**	
4.1: Entenent l'organització i el seu context	3.67	
4.1.1: Estan identificats els objectius del SGS Sistema de Gestió de la Seguretat de la Informació?	4	2, 3, MI
4.1.2: S'han identificat les qüestions internes i externes relacionades amb la seguretat de la informació?	4	2, 3, MI
4.1.3: S'han identificat com les parts internes i externes poden suposar amenaces o riscos per a la seguretat de la informació?	3	2, 3, MI
4.2: Expectatives de les parts interessades	3.67	
4.2.1: S'han identificat les parts interessades?	3	2, 3, MI
4.2.2: Hi ha un llistat de requisits sobre Seguretat de la Informació de les parts interessades?	4	2, 3, MI
4.2.3: Hi ha un llistat de requisits sobre Seguretat de la Informació referent a reglaments, requisits legals i requisits contractuals?	4	2, 3, MI
4.3: Abast del SGSI	3.00	
4.3.1: S'ha determinat l'abast del SGS i se'n conserva informació documentada?	3	2, 3, MI
4.4: Sistema de Gestió de la Seguretat de la informació	5.00	
4.4.1: El sistema de Gestió de Seguretat de la informació SGSI està establert, implementat i es revisa de manera planificada considerant oportunitats de millora?	5	2, 3
5: Lideratge	**3.83**	
5.1: Lideratge i compromís	4.00	

Requisits	Nivell de maduresa	Projectes que el milloren
5.1.1: S'han establert objectius de la Seguretat de la Informació d'acord amb els objectius del negoci?	4	2, 3, MI
5.1.2: La direcció proveeix dels recursos materials i humans necessaris per al compliment dels objectius del SGSI?	4	2, 3
5.1.3: La direcció revisa directament l'eficàcia de l'SGSI per garantir que es compleixen els objectius de l'SGSI?	4	2, 3
5.2: Política de la Seguretat de la Informació	3.50	
5.2.1: S'ha definit una política de seguretat de la informació?	4	2, 3, MI
5.2.2: S'ha establert un marc que permeti establir objectius?	2	2, 3
5.2.3: S'ha comunicat la política de seguretat de la informació a les parts interessades i a tota l'empresa?	4	1, 2, 3
5.2.4: Es manté informació documentada de la política de l'SGSI i dels seus objectius?	4	2, 3, MI
5.3: Rols i Responsabilitats	4.00	
5.3.1: S'han assignat les responsabilitats i les autoritats sobre la Seguretat de la Informació?	4	2, 3, MI
5.3.2: S'han comunicat convenientment les responsabilitats i les autoritats per a la Seguretat de la Informació?	4	1, 2, 3
6: Planificació	**3.26**	
6.1: Tractament de Riscos i Oportunitats	3.20	
6.1.1: El pla per abordar riscos i oportunitats considera les expectatives de les parts interessades en relació amb la seguretat de la informació?	2	2, 3
6.1.2: S'identifiquen i analitzen els riscos mitjançant un mètode d'avaluació i d'acceptació de riscos?	4	2, 3, MI
6.1.3: S'ha definit un procés de tractament de riscos?	2	2, 3
6.1.4: S'han establert criteris per elaborar una declaració d'aplicabilitat?	4	2, 3, MI
6.1.5: Es manté informació documentada dels punts anteriors?	4	2, 3, MI
6.2: Planificació per aconseguir objectius	3.33	
6.2.1: S'han establert objectius de la Seguretat de la Informació mesurables i d'acord amb els objectius del negoci?	4	2, 3, MI
6.2.2: Els objectius de la Seguretat de la Informació estan planificats mitjançant? - Assignació de responsabilitats - Cronograma d'execució temporal - Mètode d'avaluació	2	2, 3
6.2.3: S'han integrat els objectius de la Seguretat de la Informació als processos de l'organització tenint en compte les funcions principals dins de	4	2, 3, 4

Requisits	Nivell de maduresa	Projectes que el milloren
l'Organització?		
7: Suport	**3.43**	
7.1: Recursos	4.00	
7.1.1: S'identifiquen i assignen els recursos necessaris per a l'SGSI?	4	2, 3
7.2: Competència	2.50	
7.2.1: S'avalua la competència en matèries de seguretat de la informació per a persones que efectuen tasques que puguin afectar la seguretat?	4	2, 3, 4
7.2.2: Es manté informació actualitzada sobre la competència del personal?	1	2, 3
7.3: Conscienciació	4.00	
7.3.1: El personal està involucrat i és conscient del seu paper a la Seguretat de la Informació?	4	1, 2, 3
7.3.2: Hi ha consciència dels danys que es poden produir de no seguir les pautes de la Seguretat de la Informació?	4	1, 2, 3
7.4: Comunicació	4.00	
7.4.1: Es comunica la política de la Seguretat de la Informació amb les responsabilitats de cadascú?	4	1, 2, 3
7.4.2: Hi ha un procés per comunicar les deficiències o males pràctiques en la seguretat de la informació?	4	1, 2, 3
7.5: Informació Documentada	2.67	
7.5.1: Es disposa de la documentació requerida per la norma més la requerida per l'organització incloent-hi? - La política de la seguretat de la informació i l'abast del sistema de gestió - Els processos principals de la seguretat de la informació - Els documents exigits per la Norma ISO 27001 incloent registres - Els documents propis de seguretat de la informació identificats per l'empresa (instruccions tècniques etc.)	4	2, 3, MI
7.5.2: Hi ha un control documental on es verifica? - Qui publica el document - Qui ho autoritza i com es revisen - Formats i Suports de publicació - El seu emmagatzematge i protecció	2	2, 3
7.5.3: Es controlen els documents d'origen extern?	2	2, 3
8: Operació	**3.22**	
8.1: Control Operacional	3.00	
8.1.1: Els processos de seguretat de la informació estan documentats per controlar que es realitzen segons el planificat?	2	2, 3
8.1.2: Hi ha un procés per avaluar els riscos a la Seguretat de la Informació	4	2, 3, 4

Requisits	Nivell de maduresa	Projectes que el milloren
abans de realitzar canvis en el Sistema de Gestió o processos de Seguretat?		
8.1.3: S'estableixen mesures i plans per mitigar els riscos a la Seguretat de la Informació davant de canvis realitzats?	2	2, 3
8.1.4: S'identifiquen i es controlen els processos externalitzats quant als riscos per a la Seguretat de la Informació?	4	2, 3, 4
8.2: Anàlisi de riscos de la Seguretat de la Informació	4.00	
8.2.1: S'ha establert un procés documentat d'anàlisi i d'avaluació de riscos per a la seguretat de la informació on s'identifiqui? - El propietari del risc - La importància del risc o nivell d'impacte - La probabilitat d'ocurrència	4	2, 3, MI
8.3: Tractament de riscos de la Seguretat de la Informació	2.67	
8.3.1: S'ha implementat un pla de tractament de risc on? - Els propietaris del risc estan informats i han aprovat el pla - Es documenten els resultats	2	2, 3
8.3.2: S'identifiquen tots els controls necessaris per mitigar el risc justificant-ne l'aplicació?	3	2, 3, MI
8.3.3: Es documenta el nivell d'aplicació de tots els controls que cal aplicar?	3	2, 3, MI
9: Avaluació de l'exercici	**4.12**	
9.1: Seguiment i mesurament	4.50	
9.1.1: S'ha establert un procés continu de monitorització dels aspectes clau de la seguretat de la informació tenint en compte els controls per a la seguretat de la informació?	4	2, 3, MI
9.1.2: S'ha establert un procés documentat per avaluar els resultats dels mesuraments i que aquests resultats són presos en compte pels responsables tant dels processos com de la Seguretat de la informació?	5	2, 3, MI
9.2: Auditories Internes	4.00	
9.2.1: S'ha establert una programació d'auditories internes i assignat responsables?	4	2, 3, MI
9.2.2: L'abast i els requisits s'han definit per a l'informe d'auditoria?	4	2, 3, MI
9.2.3: Es consideren accions correctives i propostes de canvi als informes d'auditoria?	4	2, 3, MI
9.3: Informe de Revisió per la Direcció	4.00	
9.3.1: Hi ha una programació per als informes de la direcció i hi ha constància de la seva realització periòdica?	4	2, 3, MI
9.3.2: Es documenten els resultats dels informes i la direcció s'implica tant en el coneixement com en la presa de decisions sobre els aspectes crucials	4	2, 3

Requisits	Nivell de maduresa	Projectes que el milloren
per al SGSI?		
10: Millora	**3.00**	
10.1: No Conformitats i accions correctives	2.00	
10.1.1: Hi ha un procediment documentat per identificar i registrar les no-conformitats i el seu tractament?	4	2, 3, MI
10.1.2: Dins de les accions correctives hi ha una diferenciació entre accions correctives sobre la no-conformitat i sobre les causes de la mateixa?	0	2, 3
10.2: Millora continua	4.00	
10.2.1: Hi ha un procés per garantir la millora contínua de l'SGSI identificant les oportunitats de millora?	4	2, 3, MI

Taula 48: Evolució del CMM sobre els requisits de la ISO/IEC 27001 després dels projectes

La millora dels nivells de maduresa dels requisits de la norma ISO/IEC 27001, gràcies a l'implementació de les diferents propostes de projecte, queden reflectits en detall en la taula 48. Una altra manera de visualitzar aquesta millora és amb l'evolució del gràfic de maduresa general, en forma d'anàlisi GAP.

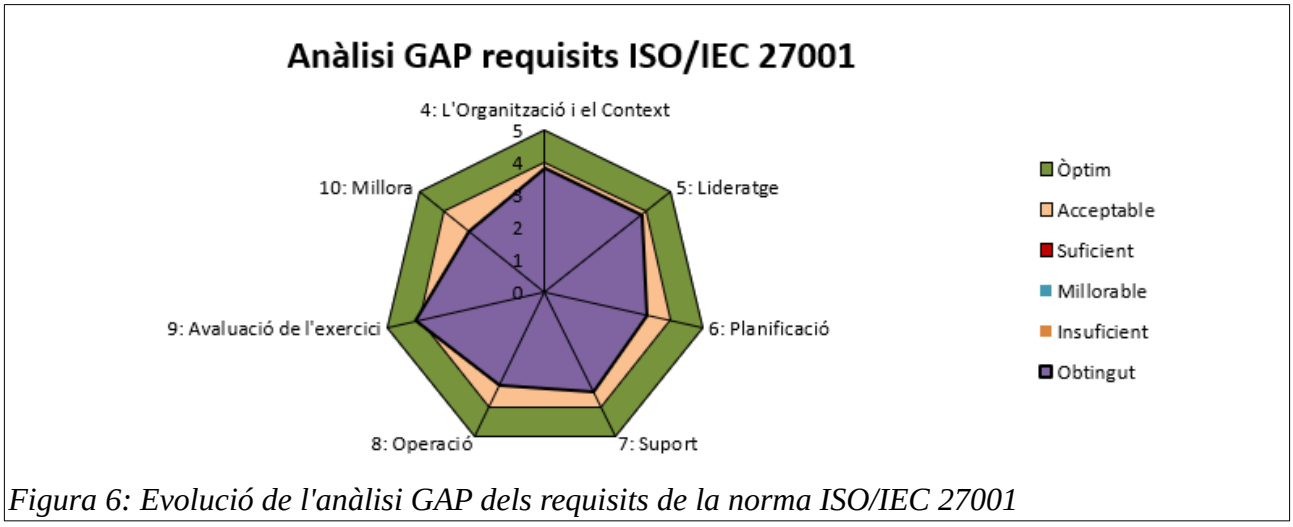


Figura 6: Evolució de l'anàlisi GAP dels requisits de la norma ISO/IEC 27001

Si es comparen el gràfic de la figura 6 amb el gràfic definit prèviament a la realització dels projectes – veure figura 3 de l'anàlisi de compliment inicial de la norma –, s'observa una millora en tots els aspectes de la norma.

En els anteriors apartats queda detallat quins projectes contribueixen a millorar cadascun dels requisits de la norma. A continuació es mostren, de forma molt resumida i per a facilitar

un anàlisi ràpid, les millores dels requisits de la norma com a conseqüència de l'aplicació de cadascun dels projectes proposats.

- **Projecte 1 (campanyes)**: afavoreix la comunicació de tots aquella informació relacionada amb la seguretat de la informació dins de l'Organització. A més, millora la consciència global sobre la importància de la mateixa.

- **Projecte 2 (indicadors)**: establir i gestionar indicadors possibilita els processos de monitorització i avaluació de resultats. És imprescindible per a fer evolucionar els requisits a un nivell de maduresa 4 (GESTIONAT I MESURABLE).

- **Projecte 3 (revisions)**: l'establiment de revisions periòdiques comporta la implicació de la direcció en l'avaluació de l'estat actual i presa de decisions sobre mesures que afecten l'SGSI de l'Organització. És imprescindible com a base de la millora continua de l'SGSI.

- **Projecte 4 (*Security by Design*)**: millora el nivell de seguretat general de l'Organització, tant a nivell tècnic com a nivell organitzatiu, en tant en quan es consideren aspectes de seguretat de la informació des de fases inicials de qualsevol nou producte o procés.

- **Millores intrínseques**: la redacció del pla director de seguretat de l'Organització aporta moltes millores. Alguns exemples són: identificació d'objectius, requisits i parts interessades; identificació d'actius i anàlisi de riscos; elaboració d'una declaració d'aplicabilitat de controls; i la redacció de documentació necessària per a implementar processos de millora (e.g. revisions i auditories).

7.8 Evolució del compliment dels controls ISO/IEC 27002 després dels projectes

En la següent taula es mostra quina seria l'evolució del compliment dels controls definits a ISO/IEC 27002, per part de l'Organització, si apliquéssim els projectes proposats en els apartats 7.1 , 7.2 , 7.3 i 7.4 , alhora que considerant les millores intrínseques (MI) per l'elaboració del pla director de seguretat 7.5 .

Control	Nivell de maduresa	Projectes que el milloren
A.5: Polítiques de seguretat de la informació	**4.00**	
A.5.1: Directrius de gestió de la seguretat de la informació	4.00	
A.5.1.1: Polítiques per la seguretat de la informació	4	2, 3, MI

Control	Nivell de maduresa	Projectes que el milloren
A.5.1.2: Revisió de les polítiques per la seguretat de la informació	4	2, 3, MI
A.6: Organització de la seguretat de la informació	**3.50**	
A.6.1: Organització interna	3.00	
A.6.1.1: Rols i responsabilitats en seguretat de la informació	4	2, 3, MI
A.6.1.2: Segregació de tasques	4	2, 3, MI
A.6.1.3: Contacte amb les autoritats	1	2, 3
A.6.1.4: Contacte amb grups d'interès especial	2	2, 3
A.6.1.5: Seguretat de la informació en la gestió de projectes	4	2, 3, 4
A.6.2: Els dispositius mòbils i el teletreball	4.00	
A.6.2.1: Política de dispositius mòbils	4	2, 3, MI
A.6.2.2: Teletreball	4	2, 3, MI
A.7: Seguretat relativa als recursos humans	**3.67**	
A.7.1: Abans del treball	4.00	
A.7.1.1: Investigació d'antecedents	4	2, 3, MI
A.7.1.2: Condicions de treball	4	2, 3, MI
A.7.2: Durant el treball	3.00	
A.7.2.1: Responsabilitats de gestió	4	1, 2, 3
A.7.2.2: Conscienciació, educació i capacitació en seguretat de la informació	4	1, 2, 3
A.7.2.3: Procés disciplinari	1	2, 3
A.7.3: Finalització del treball o canvi de lloc de treball	4.00	
A.7.3.1: Responsabilitats davant la finalització o canvi	4	2, 3, MI
A.8: Gestió d'actius	**2.44**	
A.8.1: Responsabilitat sobre els actius	3.00	
A.8.1.1: Inventari d'actius	4	2, 3, MI
A.8.1.2: Propietat dels actius	4	2, 3, MI
A.8.1.3: Ús acceptable dels actius	2	2, 3
A.8.1.4: Devolució d'actius	2	2, 3
A.8.2: Classificació de la informació	2.67	
A.8.2.1: Classificació de la informació	4	2, 3, MI
A.8.2.2: Etiquetat de la informació	2	2, 3
A.8.2.3: Manipulació de la informació	2	2, 3

Control	Nivell de maduresa	Projectes que el milloren
A.8.3: Manipulació dels suports	1.67	
A.8.3.1: Gestió de suports extraïbles	2	2, 3
A.8.3.2: Eliminació de suports	2	2, 3
A.8.3.3: Suports físics en trànsit	1	2, 3
A.9: Control d’accés	**3.58**	
A.9.1: Requisits de negoci pel control d’accés	4.00	
A.9.1.1: Política de control d’accés	4	2, 3, MI
A.9.1.2: Accés a les xarxes i als servidors de xarxa	4	2, 3, MI
A.9.2: Gestió d’accés d’usuari	3.33	
A.9.2.1: Registre i baixa d’usuari	4	2, 3, MI
A.9.2.2: Provisió d’accés d’usuari	4	2, 3, MI
A.9.2.3: Gestió de privilegis d’accés	2	2, 3
A.9.2.4: Gestió de la informació secreta d’autenticació dels usuaris	2	2, 3
A.9.2.5: Revisió dels drets d’accés d’usuari	4	2, 3, MI
A.9.2.6: Retirada o reassignació dels drets d’accés	4	2, 3, MI
A.9.3: Responsabilitats de l’usuari	4.00	
A.9.3.1: Ús de la informació secreta d’autenticació	4	2, 3, MI
A.9.4: Control d’accés a sistemes i aplicacions	3.00	
A.9.4.1: Restricció de l’accés a la informació	2	2, 3
A.9.4.2: Procediments d’inici de sessió	4	2, 3, MI
A.9.4.3: Sistema de gestió de contrasenyes	4	2, 3, MI
A.9.4.4: Ús d’utilitats amb privilegis del sistema	4	2, 3, MI
A.9.4.5: Control d’accés al codi font dels programes	1	2, 3
A.10: Criptografia	**4.00**	
A.10.1: Controls criptogràfics	4.00	
A.10.1.1: Política d’usos dels controls criptogràfics	4	2, 3, MI
A.10.1.2: Gestió de claus	4	2, 3, MI
A.11: Seguretat física i de l’entorn	**3.93**	
A.11.1: Àrees segures	4.00	
A.11.1.1: Perímetre de seguretat física	4	2, 3, MI
A.11.1.2: Controls físics d’entrada	4	2, 3
A.11.1.3: Seguretat d’oficines, despatxos i recursos	0*	n/a

Control	Nivell de maduresa	Projectes que el milloren
A.11.1.4: Protecció contra les amenaces externes i ambientals	4	2, 3, MI
A.11.1.5: El treball en àrees segures	0*	n/a
A.11.1.6: Àrees de càrrega i descàrrega	0*	n/a
A.11.2: Seguretat dels equips	3.86	
A.11.2.1: Emplaçament i protecció d'equips	4	2, 3, MI
A.11.2.2: Instal·lacions de subministrament	4	2, 3, MI
A.11.2.3: Seguretat del cablejat	4	1, 2, 3
A.11.2.4: Manteniment dels equips	4	2, 3, MI
A.11.2.5: Retirada de materials propietat de la empresa	0*	n/a
A.11.2.6: Seguretat dels equips fora de les instal·lacions	4	2, 3, MI
A.11.2.7: Reutilització o eliminació segura d'equips	2	2, 3
A.11.2.8: Equip d'usuari desatès	4	1, 2, 3
A.11.2.9: Política de lloc de treball ordenat i pantalla neta	1*	n/a
A.12: Seguretat de les operacions	**3.14**	
A.12.1: Procediments i responsabilitats operacionals	2.75	
A.12.1.1: Documentació de procediments d'operació	2	2, 3
A.12.1.2: Gestió de canvis	1	2, 3
A.12.1.3: Gestió de capacitats	4	2, 3, MI
A.12.1.4: Separació dels recursos de desenvolupament, prova i operació	4	2, 3, 4, MI
A.12.2: Protecció contra software maliciós (*malware*)	2.00	
A.12.2.1: Controls contra el codi maliciós	2	2, 3
A.12.3: Còpies de seguretat	4.00	
A.12.3.1: Còpies de seguretat de la informació	4	2, 3, MI
A.12.4: Registres i supervisió	2.25	
A.12.4.1: Registre d'events	2	2, 3
A.12.4.2: Protecció de la informació del registre	1	2, 3
A.12.4.3: Registres d'administració i operació	2	2, 3
A.12.4.4: Sincronització del rellotge	4	2, 3, MI
A.12.5: Control del software en explotació	4.00	
A.12.5.1: Instal·lació del software en explotació	4	2, 3, 4
A.12.6: Gestió de la vulnerabilitat tècnica	3.00	
A.12.6.1: Gestió de les vulnerabilitats tècniques	2	2, 3

Control	Nivell de maduresa	Projectes que el milloren
A.12.6.2: Restricció en la instal·lació de software	4	1, 2, 3
A.12.7: Consideracions sobre l'auditoria de sistemes d'informació	4.00	
A.12.7.1: Controls d'auditoria de sistemes d'informació	4	2, 3
A.13: Seguretat de les comunicacions	**4.00**	
A.13.1: Gestió de la seguretat de xarxes	4.00	
A.13.1.1: Controls de xarxa	4	2, 3, MI
A.13.1.2: Seguretat dels serveis de xarxa	4	2, 3, 4
A.13.1.3: Segregació en xarxes	4	2, 3, 4
A.13.2: Intercanvi d'informació	4.00	
A.13.2.1: Polítiques i procediments d'intercanvi d'informació	4	2, 3, MI
A.13.2.2: Acords d'intercanvi d'informació	4	2, 3, MI
A.13.2.3: Missatgeria electrònica	4	2, 3, MI
A.13.2.4: Acords de confidencialitat o no revelació	4	2, 3, MI
A.14: Adquisició, desenvolupament i manteniment dels sistemes d'informació	**3.04**	
A.14.1: Requisits de seguretat en els sistemes d'informació	4.00	
A.14.1.1: Anàlisi de requisits i especificacions de seguretat de la informació	4	2, 3, 4
A.14.1.2: Assegurar els serveis d'aplicacions en xarxes públiques	4	2, 3, MI
A.14.1.3: Protecció de les transaccions de serveis d'aplicacions	4	2, 3, 4
A.14.2: Seguretat en el desenvolupament i en els processos de suport	3.11	
A.14.2.1: Política de desenvolupament segur	4	2, 3, 4
A.14.2.2: Procediment de control de canvis en sistemes	2	2, 3
A.14.2.3: Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu	2	2, 3
A.14.2.4: Restriccions als canvis als paquets de software	2	2, 3
A.14.2.5: Principis d'enginyeria de sistemes segurs	4	2, 3, 4
A.14.2.6: Entorn de desenvolupament segur	4	2, 3, 4
A.14.2.7: Externalització del desenvolupament de software	2	2, 3
A.14.2.8: Proves funcionals de seguretat de sistemes	4	2, 3, 4
A.14.2.9: Proves d'acceptació de sistemes	4	2, 3, 4
A.14.3: Dades de prova	2.00	
A.14.3.1: Protecció de les dades de prova	2	2, 3

Control	Nivell de maduresa	Projectes que el milloren
A.15: Relació amb proveïdors	**2.67**	
A.15.1: Seguretat en les relacions amb proveïdors	2.33	
A.15.1.1: Política de seguretat de la informació en les relacions amb els proveïdors	4	2, 3, MI
A.15.1.2: Requisits de seguretat en contractes amb tercers	2	2, 3
A.15.1.3: Cadena de subministrament de tecnologia de la informació i de les comunicacions	1	2, 3
A.15.2: Gestió de la provisió de serveis del proveïdor	3.00	
A.15.2.1: Control i revisió de la provisió de serveis del proveïdor	4	2, 3
A.15.2.2: Gestió de canvis en la provisió del servei del proveïdor	2	2, 3
A.16: Gestió d'incidents de seguretat de la informació	**3.43**	
A.16.1: Gestió d'incidents de seguretat de la informació i millores	3.43	
A.16.1.1: Responsabilitats i procediments	4	2, 3, MI
A.16.1.2: Notificació dels events de seguretat de la informació	4	1, 2, 3
A.16.1.3: Notificació de punts dèbils de la seguretat	4	1, 2, 3
A.16.1.4: Avaluació i decisió sobre els events de seguretat de la informació	4	2, 3
A.16.1.5: Resposta a incidents de seguretat de la informació	2	2, 3
A.16.1.6: Aprenentatge dels incidents de seguretat de la informació	5	2, 3
A.16.1.7: Recopilació d'evidències	1	2, 3
A.17: Aspectes de seguretat de la informació per a la gestió de la continuïtat del negoci	**3.67**	
A.17.1: Continuïtat de la seguretat de la informació	3.33	
A.17.1.1: Planificació de la continuïtat de la seguretat de la informació	2	2, 3
A.17.1.2: Implementar la continuïtat de la seguretat de la informació	4	2, 3, MI
A.17.1.3: Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació	4	2, 3
A.17.2: Redundàncies	4.00	
A.17.2.1: Disponibilitat dels recursos de tractament de la informació	4	2, 3, MI
A.18: Compliment	**3.70**	
A.18.1: Compliment dels requisits legals i contractuals	3.40	
A.18.1.1: Identificació de la legislació aplicable i dels requisits contractuals	4	2, 3, MI
A.18.1.2: Drets de propietat intel·lectual (DPI)	4	2, 3, MI

Control	Nivell de maduresa	Projectes que el milloren
A.18.1.3: Protecció dels registres de la organització	1	2, 3
A.18.1.4: Protecció i privacitat de la informació de caràcter personal	4	2, 3, MI
A.18.1.5: Regulació dels controls criptogràfics	4	2, 3, MI
A.18.2: Revisions de la seguretat de la informació	4.00	
A.18.2.1: Revisió independent de la seguretat de la informació	4	2, 3
A.18.2.2: Compliment de les polítiques i normes de seguretat	4	2, 3
A.18.2.3: Comprovació del compliment tècnic	4	2, 3

Taula 49: Evolució del CMM sobre els controls definits a ISO/IEC 27002 després dels projectes

*: s'ha exclòs del càlcul del nivell de maduresa aquells controls que no són d'aplicació, segons l'establert a la declaració d'aplicabilitat de l'Organització – veure annex 18. .

La millora dels nivells de maduresa dels controls definits a ISO/IEC 27002, gràcies a l'implementació de les diferents propostes de projecte, queden reflectits en detall en la taula 49. Una altra manera de visualitzar aquesta millora és amb l'evolució del gràfic de maduresa general, en forma d'anàlisi GAP.

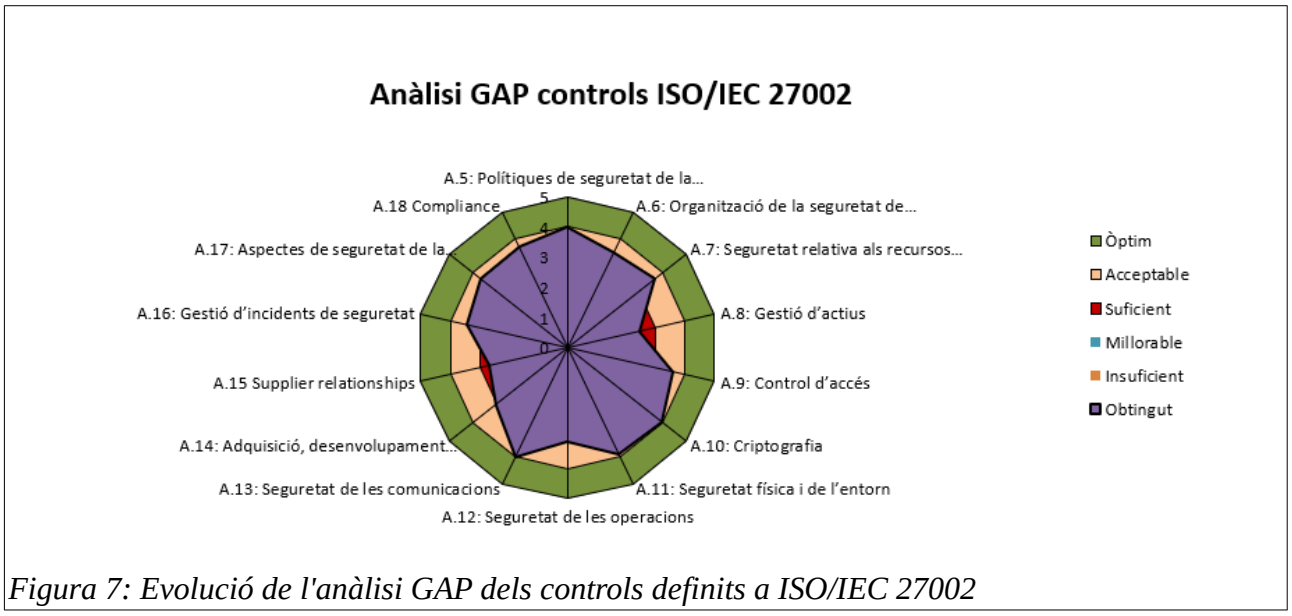


Figura 7: Evolució de l'anàlisi GAP dels controls definits a ISO/IEC 27002

Si es comparen el gràfic de la figura 7 amb el gràfic definit prèviament a la realització dels projectes – veure figura 4 de l'anàlisi de compliment inicial dels controls–, s'observa una millora en totes les categories.

Després de la implementació de tots els projectes proposats, únicament hi ha dos grups de controls que no superen el llindar 3 (DEFINIT o Acceptable):

- A.8: Gestió d'actius. No s'han definit les polítiques d'ús acceptable dels actius (o no per a tots ells) ni els procediments de devolució, així com de gestió de suports extraïbles o en trànsit i d'eliminació d'aquests. D'altra banda, no es pot garantir el tractament de la informació segons la classificació definida, ja que manquen procediments d'etiquetat i manipulació de la informació.

- A.15: Relació amb proveïdors. No s'han definit els requisits ni els mecanismes de seguretat a seguir en el subministrament de tecnologia per part de proveïdors de serveis. A més, tot i que hi ha un control de la provisió del servei, no s'efectua una gestió de canvis de forma procedimentada, en matèria de seguretat de la informació.

El detall sobre com afavoreix cada projecte a l'evolució de la maduresa de cada control es pot desprendre dels capítols corresponents – veure 7.1.4 , 7.2.4 , 7.3.4 , 7.4.4 i 7.5.3 . La visió global de la millora dels projecte, a mode resum, es troba definida en l'anàlisi de l'evolució de la norma – veure 7.7 .

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

Un element fonamental per a avaluar la maduresa de la seguretat de l'Organització és la realització d'auditories, enteses com a revisions periòdiques i exhaustives de l'SGSI de l'Organització, i en base al nivell de maduresa dels requisits definits a la norma internacional ISO/IEC 27001, així com dels controls de seguretat definits a l'ISO/IEC 27002. Amb la finalitat de conèixer-ne l'estat actual, s'ha realitzat una auditoria interna sobre l'SGSI de l'Organització amb les següents característiques:

- L'auditoria de compliment s'ha realitzat durant els dies 9, 10 i 11 de maig de 2022.
- El responsable de l'auditoria és el CISO de l'Organització.
- Les diferents activitats d'avaluació de l'SGSI s'han realitzat mitjançant una col·laboració conjunta per part del CISO de l'Organització i de l'*IT Manager*. En ambdós casos hi ha hagut el suport de treballadors de l'àrea corresponent.
- L'auditoria es centra en els processos de negoci determinats al pla director de seguretat de l'Organització.
- L'estat de l'SGSI auditat és l'existent un cop han estat aplicades les diferents propostes de projectes descrites a 7. .

Els resultats exhaustius de l'auditoria es poden consultar a l'annex 19. . A mode resum, a continuació es llisten de forma esquemàtica els punts fonamentals:

- S'han auditat tots els controls aplicables als processos de negoci de l'Organització, segons es defineix a la declaració d'aplicabilitat – veure 19.4.5 per a més detalls.
- S'ha auditat l'estat de cadascun dels requisits de seguretat de la norma ISO/IEC 27001 – veure 19.4.7 per a més detalls.
- S'ha auditat el compliment dels objectius de seguretat definits a la política de seguretat de la informació de l'Organització – veure 19.4.6 per a més detalls.
- No s'ha detectat cap no-conformitat major.
- S'han detectat un conjunt de no-conformitats menors, corresponents a tots aquells controls i requisits de la norma ISO/IEC amb nivells de maduresa actuals de 0, 1 i 2 – veure 19.4.8 per a més detalls.

- S’han efectuat un conjunt de recomanacions de millora, entre les que es destaca la perseverança en la realització d’avaluacions i revisions, l'estandarització de procediments per als diferents projectes i proveïdors, i l’adopció de bones pràctiques descrites al marc de treball ITIL [26] – veure 19.4.9 per a més detalls.

9. Conclusions

La realització del present treball ha permès avaluar la situació de l'empresa analitzada («l'Organització») en matèria de seguretat de la informació, de la forma més objectiva possible i utilitzant mecanismes reconeguts de forma internacional (els estàndards ISO/IEC i la metodologia de gestió de riscos Magerit). Aquest anàlisi exhaustiu ha estat possible gràcies a les pautes de guiatge de l'assignatura de màster «TFM - Sistemes de gestió de la seguretat de la informació» de la UOC.

Com a conseqüència dels aspectes identificats en l'anàlisi de la situació inicial, s'han pogut realitzar propostes per a millorar l'estat general de la seguretat de la informació de l'Organització, en forma de mesures tècniques i organitzatives. Els projectes proposats, tot i partir d'una naturalesa teòrica, tant en la seva planificació temporal com econòmica, poden servir de base per a desenvolupar-los i implementar-los de forma real en l'àmbit de l'Organització. La redacció del present treball per si mateixa ha permès, a més, fer evolucionar l'estat existent de l'SGSI, per exemple amb la definició de documentació i procediments, que podrien ésser utilitzats de forma operativa.

Dels punts esmentats anteriorment es desprèn que la realització del present treball ha permès la consecució dels objectius fixats inicialment, els quals es poden trobar definits a 1.2 .

10. Glossari

ARO: *Annual Rate of Occurrence*
CISO: *Chief information security officer*
CMM: *Capability Maturity Model*
CPD: *Centre de Processament de Dades*
DMZ: *Demilitarized Zone*
FTP: *File Transfer Protocol*
GDPR: *General Data Protection Regulation*
HTTP: *Hypertext Transfer Protocol*
IEC: *International Electrotechnical Commission*
ISA: *Interconnection Security Agreement*
ISO: *International Organization for Standarization*
IT: *Information Technology*
ITIL: *Information Technology Infrastructure Library*
LOPDGDD: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
Magerit: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MoM: *Minutes of Meeting*
NTP: *Network Time Protocol*
RRHH: Recursos humans
SGSI: Sistema de Gestió de la Seguretat de la Informació
SLA: *Service Level Agreement*
UPS: *Uninterruptible power supply*
UTC: *Universal Time Coordinated*
VPN: *Virtual Private Network*

11. Bibliografia

[1] **UOC** (2017). *UNE-EN ISO/IEC 27002*. Disponible a: https://www.campus.uoc.edu/biblioteca/prestatgeries/articles/protegits/B2627/027002NEII100_ES.pdf (última consulta: 26/02/2022)

[2] **UOC** (2022). Checklist per a l'ANNEX A ISO 27001. Posat a disposició com a part del material del TFM

[3] **AENOR FORMACION** (2017, maig). *UNE-EN ISO/IEC 27001*. Posat a disposició com a part del material del TFM

[4] **UOC** (2022). Checklist per a la norma ISO 27001. Posat a disposició com a part del material del TFM

[5] **UOC** (2021). Correccions i solucions de PACs de l'assignatura *M1.709 – Sistemes de gestió de la seguretat*

[6] **UOC** (2022). Guia de redacció del TFM en Sistemes de Gestió de la Seguretat de la Informació

[7] **Organització** (2001). Política de seguretat

[8] **UOC** (2020, setembre). Mòdul Anàlisi de riscos de l'assignatura *M1.709 – Sistemes de gestió de la seguretat*

[9] **UOC** (2020, setembre). Mòdul Implantació d'un SGSI de l'assignatura *M1.709 – Sistemes de gestió de la seguretat*

[10] **UOC** (2020, setembre). Mòdul *Desenvolupament d'alguns objectius de control de l'SGSI de l'assignatura M1.709 – Sistemes de gestió de la seguretat*

[11] **27001 Academy** (2014, setembre). I*nforme: Lista de documentación obligatoria requerida por ISO/IEC 27001*. Posat a disposició com a part del material del TFM

[12] **Consejo Superior de Administración Electrónica** (2012). Metodologia MAGERIT, versió 3. *Libro I – Método*. Disponible a: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html (última consulta: 17/03/2022)

[13] **Consejo Superior de Administración Electrónica** (2012). Metodologia MAGERIT, versió 3. *Libro II – Catálogo de Elementos*. Disponible a:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html (última consulta: 17/03/2022)

[14] **Consejo Superior de Administración Electrónica** (2012). Metodologia MAGERIT, versió 3. *Libro III – Guía de Técnicas*. Disponible a: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html (última consulta: 17/03/2022)

[15] https://www.pilar-tools.com/es/glossary/index.html?n=DependenciasEntreActivos.html (última consulta: 25/03/2022)

[16] **UNINETT** (2010). *UFS126: Informasjonsikkerhetspolicy*. Disponible a: https://www.uninett.no/sites/default/files/webfm/UFS%20126.pdf (última consulta: 06/03/2022)

[17] **Goldsmiths, University of London** (2021). *Information Security Policy*. Disponible a: https://www.gold.ac.uk/media/docs/it/Information-Security-Policy.pdf (última consulta: 07/03/2022)

[18] **Reguvis** (2021). *IT-Grundschutz-Kompendium*. Disponible a: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf

[19] https://isowin.org/blog/politica-seguridad-ISO-27001/ (última consulta: 05/03/2022)

[20] https://www.worldsensing.com/de/quality-and-security-policy/ (última consulta: 06/03/2022)

[21] https://www.isms.online/iso-27001/information-security-policy/ (última consulta: 07/03/2022)

[22] https://www.isms.online/iso-27001/annex-a-5-information-security-policies/ (última consulta: 07/03/2022)

[23] **itgovernance** (2021). *The importance of the Statement of Applicability in ISO 27001*. Disponible a: https://www.itgovernance.co.uk/blog/the-importance-of-the-statement-of-applicability-in-iso-27001 (última consulta: 26/02/2022)

[24] **itgovernance** (2021). *ISO 27001 management review: a practical guide*. Disponible a: https://www.itgovernance.co.uk/blog/iso-27001-management-review-a-practical-guide (última consulta: 11/03/2022)

[25] **INFOSAVVY** (2022). *ISO 27001 Clause 9.1 Performance evaluation Monitoring, measurement, analysis & evaluation*. Disponible a: https://info-savvy.com/iso-27001-clause-9-1-performance-evaluation-monitoring-measurement-analysis-and-evaluation/ (última consulta: 12/03/2022)

[26] **IBM** (2019). *IT Infrastructure Library (ITIL)*. Disponible a: https://www.ibm.com/cloud/learn/it-infrastructure-library (última consulta: 11/05/2022)

12. Annex I: Política de Seguretat de la Informació

Control de versions

Versió	Data	Descripció dels canvis
V1	09/03/2022	Versió inicial del document

12.1 Necessitat de la política de seguretat

Per aconseguir assolir els objectius de negoci, l'Organització necessita recolzar-se en els actius i serveis de la informació. Degut a la creixent rellevància d'aquests serveis en el si de l'Organització en els darrers anys, es fa cada vegada més necessari analitzar i establir mesures que protegeixin la informació, en les dimensions clàssiques de la seguretat:

- **Confidencialitat**: la informació només és accedida per aquells qui estan legitimats per fer-ho.
- **Integritat**: la informació no ha estat modificada durant el cicle de vida, de forma il·legítima.
- **Disponibilitat**: la informació està accessible sempre que és requerida.

L'augment de la importància dels serveis de la informació, juntament amb el desenvolupament constant de noves amenaces, que se sumen a les ja existents, fa imprescindible la creació d'una política de seguretat de la informació. El present document defineix l'esmentada política, en tant en quant es fixen les directrius a seguir per a la definició i implementació d'un Sistema de Gestió de Seguretat de la Informació (o SGSI), bastant-se en les normes marcades per l'estàndard internacional ISO/IEC 27001 [3] i els controls definits a l'estàndard ISO/IEC 27002 [1].

La política de seguretat de la informació està adreçada a tots els empleats de l'Organització, així com a totes les parts interessades que hi col·laborin d'una forma o altre. En concret, la política de seguretat de la informació està també adreçada als contractistes, proveïdors i terceres entitats que treballin per a o amb l'Organització.

12.2 Abast

La present política de seguretat de la informació aplica a:

- Tots els actius propietat de l'Organització, ja siguin físics (e.g. instal·lacions físiques, hardware) o lògics (e.g. software).
- Tots els actius propietat de tercers però dels quals se'n fa ús com a part dels processos de negoci de l'Organització (e.g. equips de xarxa).
- Tot el cicle de vida dels processos pilars de l'Organització: adquisició de dades, tractament i emmagatzematge de dades i publicació de resultats.
- Tota persona implicada en els processos pilars de l'Organització, ja siguin empleats, subcontractistes o terceres parts.
- Tota comunicació d'informació, tant de manera interna dins de l'Organització com de forma externa, sempre i quan existeixi un intercanvi d'informació cap a o des de l'Organització.

12.3 Objectius de seguretat

La informació és el punt central dels processos de l'Organització i que, per tant, cal protegir. Es defineixen els següents objectius de seguretat de la informació:

- Garantir un nivell de protecció adequat de la informació i dels actius i serveis que la sustenten.
- Garantir la continuïtat dels processos de negoci de l'Organització.
- Garantir la confidencialitat, integritat i disponibilitat de la informació de l'Organització i de totes les parts implicades en els processos de negoci.
- Assegurar el compliment del marc legal aplicable i dels contractes establerts.
- Assegurar la conformitat amb l'estàndard internacional ISO/IEC 27001 [3].
- Garantir l'aplicació de processos de millora contínua en el marc de la seguretat de la informació.
- Garantir el coneixement i aplicació de la política de seguretat de la informació per part de totes les parts interessades i de tots els empleats de l'Organització.
- Garantir la revisió periòdica de la política de seguretat de la informació per part del Comitè de seguretat.

12.4 Marc regulador

Cal assegurar el compliment del marc legal aplicable, així com de tots els contractes que s'hagin pogut tancar amb les diferents parts involucrades en els processos de l'Organització.

Degut a les activitats i processos duts a terme en el si de l'Organització, són d'aplicació obligatòria les següents lleis i reglaments:

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, altrament anomenat GDPR per les seves sigles en anglès (*General Data Protection Regulation*), pel qual es regula el tractament de dades personals dins de la Unió Europea. És necessari aplicar el reglament degut a que l'Organització tracta dades personals, tant d'empleats com de terceres parts.

- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, altrament anomenada LOPDGDD per les seves sigles en castellà. Aquesta llei complementa el GDPR en aquells aspectes els quals el reglament europeu deixa a decisió dels estats membres. La seva aplicació està justificada pel mateix motiu que el GDPR, però en aquest cas a nivell estatal.

- Reial Decret Legislatiu 1/1996, de 12 d'abril, amb el qual es regula la Llei de Propietat Intel·lectual. És necessari l'aplicació i compliment d'aquest reial decret per a tota aquella informació que ha estat genuïnament creada per l'Organització o per alguna de les terceres parts que hi col·laboren, alguns exemples de la qual poden ser: software utilitzat o resultat d'estudis.

- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic. El regulat per aquesta llei aplica a tots aquells serveis prestats per l'Organització cap a terceres entitats o clients, així com als serveis externalitzats per part de l'Organització a contractistes i proveïdors de serveis de la societat de la informació.

- Altres regulacions equiparables a les espanyoles i d'aplicació obligatòria en altres països de la Unió Europea amb els quals treballa l'Organització.

- Contractes establerts entre l'Organització i terceres parts per a la provisió de serveis, tant en els casos en que l'Organització actuï com a proveïdora del servei com en aquells casos en que aquesta subcontracta el servei i n'és, per tant, beneficiària final.

12.5 Rols i responsabilitats

Existeixen rols definits amb responsabilitats associades, en l'àmbit de la seguretat de la informació de l'Organització. Degut a la naturalesa internacional de l'Organització, els rols tenen associada també una nomenclatura internacional, en anglès.

A continuació es mostra una breu descripció dels rols existents. Es pot consultar el detall del conjunt de responsabilitats i tasques associades a cadascun dels rols a Annex V: Gestió de Rols i Responsabilitats.

12.5.1 Cap de seguretat o *Chief information security officer* (CISO)

El CISO és un dels rols principals en l'àmbit de la seguretat de la informació. Es tracta d'una persona per a la qual la seguretat és l'eix central de les tasques que ha de realitzar dins de l'Organització, i que representa la màxima autoritat (i responsabilitat) en aquesta àrea, juntament amb la direcció de la Organització.

12.5.2 Cap del departament de les tecnologies d'informació o *IT Manager*

La persona que ocupa el rol d'*IT Manager* s'encarrega de gestionar i coordinar tots els temes relacionats amb els actius d'IT (de l'anglès *Information Technology)*, fent referència tant als actius físics (e.g. servidors de dades o equips de xarxa) com als actius lògics (e.g. software).

Tot i que la seguretat de la informació no és el seu objectiu prioritari, moltes de les seves responsabilitats contemplen tasques en aquest àmbit. L'*IT Manager* haurà de treballar sovint de forma conjunta amb el CISO.

12.5.3 El proveïdor de servei o *Service provider*

El proveïdor de serveis, en tant en quant està involucrat en els processos de l'Organització, te també responsabilitats de seguretat, les quals han d'estar definides en els contractes bilaterals entre el proveïdor i l'Organització.

12.5.4 Director del centre de l'Organització

La direcció de l'Organització, encapçalada formalment per la figura del director, representa la màxima autoritat (i responsabilitat) dins de l'Organització. Entre moltes altres responsabilitats, també te assignades tasques dins de l'àmbit de la seguretat de la informació, com la revisió, aprovació i difusió de la present política de seguretat de la informació.

La direcció de l'Organització treballarà sovint de forma conjunta amb el CISO i amb l'*IT Manager* en qüestions relatives a la seguretat de la informació.

12.5.5 Treballadors

Tots els treballadors de l'Organització, així com els subcontractistes, tenen associades responsabilitats en quant a la seguretat de la informació, com és complir amb les polítiques, normes i guies que estan definides per la documentació formal de l'Organització.

12.6 Declaracions de la política

En concordança amb els requisits establerts per l'estàndard internacional ISO/IEC 27001 [3], es realitzen una sèrie de declaracions en la present política de seguretat de la informació, prenent en consideració les diferents categories establertes en els controls definits a l'estàndard ISO/IEC 27002 [1].

12.6.1 Polítiques de seguretat de la informació

Queda definida la present política general de seguretat de la informació, la qual queda ampliada amb diferents polítiques i reglaments rellevants per als processos de l'Organització. Aquestes són:

- Gestió de Rols i Responsabilitats.
- Procediment d'Auditories Internes.
- Gestió d'Indicadors.
- Procediment de Revisió per Direcció.
- Metodologia d'Anàlisi de Riscos.
- Declaració d'Aplicabilitat.
- Reglament general d'accés a la xarxa de l'Organització.
- Reglament de desplegament de serveis d'informació a una xarxa accessible (DMZ).
- Política sobre ús de software a l'Organització.
- Política de desenvolupament segur.
- Política de control d'accés a la informació de l'Organització.
- Política sobre l'ús de dispositius d'usuari: portàtils, telèfons i *smartphones*.
- Política sobre actualitzacions de sistemes.
- Política sobre gestió de contrasenyes.
- Política sobre el controls criptogràfics.
- Política sobre comunicacions dins de l'Organització i amb entitats externes.
- Reglament de mecanismes de protecció d'oficines i equipament físic.
- Reglament d'ús del correu electrònic.
- Política de còpies de seguretat.
- Política sobre l'ús de serveis en el *Cloud*.
- Política sobre la regulació del teletreball.
- Política sobre la contractació i tracte amb proveïdors.
- Política sobre la classificació de la informació.

Totes les polítiques han de ser revisades periòdicament pel responsable o responsables corresponents, com a mínim un cop cada 12 mesos, o bé abans si les circumstàncies ho requereixen.

12.6.2 Organització de la seguretat de la informació

Les diferents tasques i responsabilitats en matèria de la seguretat de la informació estan assignades als diferents rols existents. Existeix una descripció detallada dels rols i les responsabilitats Annex V: Gestió de Rols i Responsabilitats, tal i com s'esmenta a 12.6.1 i 12.5 .

En el cas d'un incident de seguretat que suposi una violació o perjudici de les dades personals d'un interessat, s'avisarà a l'autoritat pertinent i es restarà a la seva disposició per a resoldre possibles consultes d'informació. Al seu torn, s'avisarà a l'interessat sense cap dilació sobre l'incident.

L'Organització, per mitjà del seu CISO, es mantindrà al dia sobre l'estat de la seguretat dels sistemes empleats, assistint en cas necessari a events de seguretats nacionals o internacionals.

Es considerarà en tot projecte nou l'aplicació del concepte de *Security by Design*.

12.6.3 Seguretat en els recursos humans

S'avaluarà la idoneïtat de contractació de cada nou empleat, incloent una revisió dels possibles antecedents penals, així com de cada subcontractista o tercera persona que treballi amb l'Organització. A més, en els contractes entre les parts hi haurà clàusules respecte a la seguretat de la informació, indicant que, en cas d'incompliment de les mateixes, hi pot haver conseqüències laborals i, segons el cas, també conseqüències administratives i penals.

Es definiran de manera clara i inequívoca els processos a seguir en el cas de baixa d'empleats, subcontractistes o terceres persones que treballin amb l'Organització.

12.6.4 Gestió d'actius

Tots els actius de l'Organització, ja siguin físics (e.g. instal·lacions físiques, hardware) o lògics (e.g. software), han d'estar inventariats i disposar d'un propietari o encarregat formal. Les normes d'ús dels actius venen marcades per la política corresponent – veure 12.6.1 per a més detalls.

La informació tractada dins de l'Organització queda emmarcada en una de les següents categories:

- **Informació pública**: tota aquella informació que pot ser accessible per tothom. En l'àmbit de projectes o estudis determinats, que sigui pública no eximeix de la necessitat de demanar-ne accés a les persones responsables (e.g. al cap de projecte).

- **Informació interna**: tota aquella informació l'ús de la qual queda restringit a un projecte, estudi, o equip de treball determinat. L'accés a la informació està regit pel principi de «necessitat de saber» (de l'anglès «*Need-to-Know*»), segons el qual la informació només s'ha de distribuir a qui necessiti saber-la.

- **Informació confidencial**: tota aquella informació especialment sensible, com per exemple dades personals, dades contractuals, o dades estratègiques per a l'Organització. Tota distribució i accés a aquesta informació ha de ser controlat, validat i registrat. En cas que l'intercanvi d'informació es produeixi amb entitats externes a l'Organització, s'haurà de fer sempre sota l'empara d'acords de confidencialitat.

12.6.5 Control d'accés

L'accés a la informació de l'Organització ha de quedar controlat segons la política corresponent – veure 12.6.1 per a més detalls. Els drets d'accés han de ser revisats periòdicament (mínim cada 12 mesos) i actualitzats en funció de les circumstàncies canviants (e.g. alta i baixa d'usuaris, o canvi d'empleats en projectes o estudis dins de l'Organització).

Els procediments d'inici de sessió (autenticació i autorització) han de ser segurs, segons els estàndards existents, i s'han de revisar periòdicament amb la finalitat de detectar possibles fallades o potencials millores. Les contrasenyes i credencials utilitzats es gestionaran de forma segura, e.g. amb un sistema de gestió de contrasenyes.

12.6.6 Criptografia

Els controls criptogràfics emprats dins de l'Organització i per a comunicacions amb entitats externes venen delimitats per la política corresponent – veure 12.6.1 per a més detalls.

12.6.7 Seguretat física i de l'entorn

Existeixen controls físics d'accés a les instal·lacions de l'Organització. Els empleats, subcontractistes o terceres persones que vulguin accedir a les oficines de l'Organització, hauran de disposar de l'acreditació corresponent.

Totes les zones de les instal·lacions de l'Organització han d'estar protegides contra amenaces externes i ambientals, segons marca el reglament corresponent – veure 12.6.1 – especialment aquelles on s'allotgen actius involucrats en processos crítics de l'Organització, o bé actius que emmagatzemen o tracten informació confidencial.

Els equips d'IT que donen suport als processos de negoci de l'Organització, tant per a l'adquisició de dades, el tractament i emmagatzematge d'aquestes, i la publicació de resultats, han de ser mantinguts segons les polítiques establertes – veure 12.6.1 per a més detalls. D'igual forma, cal garantir el subministrament ininterromput d'aquests equips.

12.6.8 Seguretat a les operacions

Existeixen procediments documentats, revisats (mínim cada 12 mesos), i amb propietari formal, respecte a les tasques realitzades durant les operacions dels processos de negoci. Aquests procediments contemplen la possibilitat de canviar els sistemes existents, així com d'ampliar-ne o reduir-ne la capacitat segons les circumstàncies.

Amb la finalitat de mantenir les propietats de la seguretat en les operacions (confidencialitat, integritat, disponibilitat), cal disposar d'entorns separats, de manera que tots els desenvolupaments i proves es realitzin de forma prèvia a les operacionalitzacions dels sistemes. És necessari també seguir la política de còpies de seguretat de l'Organització – veure 12.6.1 per a més detalls.

La informació relacionada amb els events que succeeixen en les operacions regulars s'haurà de registrar. Cal protegir, a més, l'accés a aquests registres, per poder-se tractar d'informació interna i/o confidencial.

Els sistemes d'informació s'han de revisar periòdicament, realitzant tant auditories internes (mínim cada 12 mesos) com auditories externes (mínim cada 36 mesos).

12.6.9 Seguretat a les comunicacions

L'accés a les xarxes de l'Organització queda regulat per les polítiques i reglaments referenciades a 12.6.1 , tant en el cas de les intra-comunicacions com de les inter-comunicacions.

És necessari constituir xarxes independents i separades amb mecanismes de seguretat (e.g. amb tallafocs), i que responguin als objectius pels quals han estat dissenyades. Com a exemple, hi haurà una o més xarxes d'accés public (o DMZ), connectades de manera molt

restringida a les xarxes internes de l'Organització i únicament en el sentit intern → DMZ, mai en sentit contrari.

S'han de seguir les pautes fixades en les polítiques per a l'intercanvi d'informació entre entitats – veure 12.6.1 per a més detalls. En el cas que es tracti de comunicacions on es transmet informació confidencial haurà d'existir, a més, un o més acords de confidencialitat.

12.6.10 Adquisició, desenvolupament i manteniment de sistemes d'informació

S'aplicarà la política de desenvolupament segur – veure 12.6.1 – tant en nous desenvolupaments de sistemes com en el manteniment i extensió de sistemes existents. Aquesta metodologia inclou un anàlisi previ dels requisits de seguretat, ja en les fases inicials de concepció dels sistemes (*Security by Design*).

Durant les diferents fases del desenvolupament de sistemes i, de forma prèvia a qualsevol operacionalització, es provaran els sistemes de forma íntegra, tant de manera funcional com explícitament en els requisits de seguretat definits. Aquestes fases de proves es realitzaran en entorns separats del d'operacions.

Els requisits de desenvolupament i prova apliquen tant als sistemes d'informació desenvolupats dins de l'àmbit de l'Organització, com aquells subcontractats a terceres parts.

12.6.11 Relació amb proveïdors

Existeix una política sobre la contractació i tracte amb proveïdors – veure 12.6.1 per a més detalls –, la qual fixa quines són les guies a seguir durant tota la cadena de subministrament de serveis d'informació per part de proveïdors i terceres parts.

Cal revisar periòdicament (mínim cada 12 mesos) el compliment de les pautes de relació definides, i prendre mesures per a corregir els procediments en cas que aquests no s'adeqüin a l'establert per la política corresponent.

12.6.12 Gestió d'incidents de seguretat de la informació

En l'àmbit de la seguretat de la informació es defineixen rols i responsabilitats, tal i com s'exposa a 12.5 . A més, existeixen procediments documentats sobre com respondre a incidents de seguretat, incloent la identificació i notificació dels possibles punts dèbils dels sistemes.

Cal recopilar evidències dels incidents ocorreguts, de manera similar a com es registren els events que succeeixen en les operacions regulars, de manera que s'hi pugui fer referència posteriorment.

Un dels objectius dels procediments de gestió d'incidents de seguretat ha de ser aprendre dels incidents, amb l'objectiu de millorar la seguretat global de l'Organització.

12.6.13 Gestió de la continuïtat del negoci

La gestió de la continuïtat del negoci és un aspecte que s'ha de planificar i documentar, de manera que les parts implicades sàpiguen com actuar en cas de desastre, com pot ser en cas de terratrèmols o incendis. Una mesura rellevant és l'implementació de redundàncies dels actius crítics dels processos de l'Organització, com poden ser els serveis d'emmagatzematge de dades i els de publicació de resultats.

Les mesures de continuïtat de la seguretat de la informació s'hauran de revisar de forma periòdica (mínim cada 12 mesos), i adaptar en cas necessari.

12.6.14 Compliment

La legislació i contractes aplicables han estat identificats i descrits a 12.4 .

El nivell de compliment de les mesures de seguretat de la informació s'haurà d'avaluar contínuament mitjançant indicadors dissenyats per a tal efecte. Periòdicament, a més, cal realitzar auditories, tant de manera interna (mínim cada 12 mesos), com de forma externa (mínim cada 36 mesos).

12.7 Tractament de desviacions i excepcions

En el cas que una part interessada que tracti amb l'Organització consideri inviable el compliment de la política, en qualsevol de les seves disposicions, serà necessari comunicar aquest fet, juntament amb les raons, al CISO de l'Organització. Aquest convocarà una reunió amb els altres membres del Comitè de seguretat, en la que s'avaluarà la situació i es decidirà si és procedent concedir una excepció.

En cas que es consideri inoportú continuar les relacions entre la part no complidora de la política i l'Organització, s'haurà de cessar de manera immediata qualsevol relació existent entre ambdues parts.

13. Annex II: Procediment d'Auditories Internes

Control de versions

Versió	Data	Descripció dels canvis
V1	16/03/2022	Versió inicial del document

13.1 Introducció

Les auditories internes són un dels mecanismes més efectius a l'hora d'avaluar d'una manera objectiva quin és l'estat actual de l'SGSI de l'Organització. La seva definició i realització són, a més, un requisit indispensable si l'Organització vol ser conforme amb el que dicta la norma ISO/IEC 27001 [3].

En el present document es defineix el procediment a seguir per a la realització d'auditories internes en l'àmbit de l'SGSI de l'Organització. A més del procediment, se'n determinen aspectes relatius a la programació temporal de l'auditoria, a la responsabilitat formal i al contingut de la mateixa.

13.2 Abast

L’abast del present document es centra en la definició de les auditories internes que es duen a terme com a avaluacions periòdiques de l’SGSI de l’Organització. Com a tal, i en concordança amb l’abast determinat al pla director de seguretat, les auditories definides se centraran en els processos definits al pla director de seguretat:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

13.3 Procediment d’auditories internes

Tal i com estableix la clàusula 9.2 de la norma ISO/IEC 27001 [3], es defineix el requisit d’efectuar auditories internes sobre l’SGSI de l’Organització, de forma periòdica. Aquestes auditories persegueixen dos objectius principals:

- Avaluar l’estat actual de l’SGSI de l’Organització i si aquest compleix amb els requisits de seguretat establerts per a la mateixa. A més, també es busca descobrir possibles nous problemes de seguretat que, fins al moment de realització de l’auditoria, hagin passat desapercebuts.

- Avaluar la conformitat de l’SGSI de l’Organització amb la norma internacional ISO/IEC 27001 [3].

De manera prèvia a la realització efectiva d’una auditoria, és necessari abordar alguns aspectes importants. En els capítols 13.3.1 , 13.3.2 i 13.3.3 es defineixen els criteris a seguir per a realitzar auditories internes dins de l’Organització.

13.3.1 Programació d’auditories internes

Les auditories internes s’han de programar de forma planificada. Tal i com marca la política de seguretat de la informació de l’Organització (veure Annex I: Política de Seguretat de la Informació), es realitzaran auditories internes amb una periodicitat màxima de 12 mesos. Aquest període temporal es podrà reduir puntualment en el cas que el CISO – o el conjunt del Comitè de seguretat de la informació – ho consideri necessari.

Un cop finalitzada l’auditoria interna corresponent, s’haurà de planificar la temporalitat de la següent, indicant la data prevista de la seva realització. Aquesta data està subjecte a modificacions fins a un màxim de 2 mesos abans de la data d’execució. Arribats a aquest punt, únicament una decisió per part de la direcció de l’Organització, amb la justificació que aquesta consideri pertinent, i previ anàlisi i acceptació de les conseqüències, pot fer canviar la data de realització de l’auditoria.

Un aspecte important a l’hora de fixar la data (i hora) de realització de l’auditoria és avaluar l’impacte que aquesta pot tenir sobre els processos de negoci de l’Organització. Tal i com s’exposa al control 12.7.1 de l’ISO/IEC 27002 [1], és recomanable limitar l’abast de les auditories, de manera que aquestes no siguin invasives. En el cas que es prevegi algun tipus d’afectació als processos operatius, caldrà acordar amb totes les parts implicades el dia i hora de les accions (e.g. amb els responsables d’operacions de tots els projectes implicats). En funció del tipus de procés afectat, serà més adequat realitzar l’auditoria fora d’horari laboral (e.g. menys afectació a usuaris que accedeixin als resultats dels estudis) o bé dins

d’hores laborals habituals (e.g. capacitat de resposta per parts dels empleats de l’Organització i contractistes).

Per a poder planificar i, posteriorment, dur a terme les auditories internes, és necessari que la direcció de l’Organització hi destini els recursos personals i econòmics necessaris.

13.3.2 Responsable de l’auditoria interna

Generalment el responsable de les auditories internes serà el CISO de l’Organització, entenent que el focus principal de les mateixes està posat en la seguretat de la informació. En el cas d’auditories internes amb un altre enfocament, es possible que s’assigni un altre responsable formal, ja sigui l’*IT Manager* o un responsable d’una altra àrea.

L’organització, preparació i execució de les auditories pot esser delegada a terceres persones, ja sigui personal intern de l’Organització (sovint dels equips de treball del CISO o bé de l’*IT Manager*), o bé personal extern. En aquest darrer cas, es poden contractar els serveis d’un o més consultors experts en matèria de seguretat que, a més, han de tenir experiència en estàndards internacionals i, més concretament, en la normativa ISO/IEC 27001 [3]. De forma similar a com es comentava anteriorment, en el cas d’auditories internes amb un enfocament que no sigui el de la seguretat de la informació, hi haurà uns altres requisits en quan a l’experiència i coneixement que ha de tenir la persona (o persones) que s’encarreguin de gestionar l’auditoria.

Cal destacar que, com a mínim, participaran 2 persones (ja siguin empleats o consultors) en l’organització, preparació i execució de les auditories internes de l’Organització. El motiu principal és la revisió mútua de la feina de l’altre, ja que un auditor mai pot auditar-se a ell mateix. Aquesta condició no exclou el fet que es puguin assignar més de 2 persones a l’auditoria, si es considera necessari.

De forma similar a com s’esmenta a 13.3.1 , la direcció ha d’assignar els recursos personals i econòmics necessaris per a possibilitar una correcta gestió de les auditories.

13.3.3 Model d’informe d’auditoria

L'informe d’auditoria ha de contenir, com a mínim, els següents elements, segons es desprèn de [9]:

- **Data**: Es tracta del dia (o dies) en que es realitza l’auditoria. En cas que sigui rellevant, cal indicar també la franja horària en que es duen a terme les activitats.

- **Responsable**: Nom del responsable de l’auditoria.

- **Nom de l’auditor o auditors**: Nom de la persona (o persones) encarregada de dur a terme l’auditoria. Pot o no coincidir amb el responsable.

- **Abast**: Cal indicar quin és l’abast de l’auditoria. Normalment aquest coincidirà amb l’abast definit al pla director de seguretat de l’Organització, és a dir, s’auditaran els processos de negoci de l’Organització rellevants per a l’SGSI.

- **Controls auditats**: Quins controls de seguretat de la informació s’analitzaran com a part de l’auditoria, d’entre tots els que apliquen a l’SGSI de l’Organització – veure Annex VII: Declaració d’Aplicabilitat pel llistat complet.

- **Conformitat de l’SGSI amb els requisits de seguretat de l’Organització**: Es tracta de verificar si es compleixen tots els requisits marcats per l’Organització, definits a Annex I: Política de Seguretat de la Informació.

- **Conformitat de l’SGSI amb la norma ISO/IEC 27001**: Es tracta de verificar si es compleixen tots els requisits definits a l’estàndard internacional ISO/IEC 27001. Per a facilitar aquest anàlisi de conformitat, existeix una *checklist*, definida a [4].

- **No-conformitats detectades**: En base a l’anàlisi de conformitat anterior, en aquest apartat es documentaran tots aquells punts que mostrin una no-conformitat amb els requisits de seguretat de l’Organització o amb la norma ISO/IEC 27001.

- **Recomanacions de millora**: Es formularan totes aquelles recomanacions de millora que puguin ajudar a reduir el número de no-conformitats.

Cal documentar tota la informació recollida, tant les conformitats com les no-conformitats, a més dels elements generals descriptius de l’auditoria interna en qüestió. Aquesta documentació s’haurà de conservar, tant per a ser revisada posteriorment, com per a evidenciar l’existència i realització de l’auditoria.

Els resultats de l’auditoria s’hauran de comunicar a la direcció de l’Organització per a que siguin revisats en l’àmbit del procediment definit a Annex IV: Procediment de Revisió per Direcció. A més, si s’escau, els resultats també seran avaluats en l’àmbit del Comitè de seguretat de la informació – veure Annex V: Gestió de Rols i Responsabilitats. En concordança amb l’esmentat a 13.3.2 , en el cas que l’auditoria tingui un enfocament diferent del de l’àmbit de seguretat de la informació, s’haurà d’informar dels resultats al responsable de l’àrea corresponent.

14. Annex III: Gestió d'Indicadors

Control de versions

Versió	Data	Descripció dels canvis
V1	12/03/2022	Versió inicial del document

14.1 Introducció

Un dels objectius fonamentals de l'SGSI de l'Organització, i tal i com està definit a la política de seguretat de la informació, és garantir que s'apliquen els processos de millora contínua, de manera que l'SGSI es mantingui sempre actualitzat. Un pas imprescindible per a poder mantenir l'SGSI en constant revisió i millora és fer ús d'indicadors, els quals possibiliten el monitoratge dels controls de seguretat establerts a l'Organització. La definició i gestió d'indicadors és, a més, un dels requisits establerts per la norma ISO/IEC 27001 [3], concretament en la seva clàusula 9.1 (seguiment, mesurament, anàlisi i avaluació).

En el present document es descriu l'estructura dels indicadors que es fan servir a l'hora de mesurar els controls de seguretat establerts – veure Annex VII: Declaració d'Aplicabilitat per al llistat complet dels controls que apliquen als processos de negoci de l'Organització, d'entre tots els definits a l'ISO/IEC 27002 [1]. A més, també es defineix quin són els mètodes de seguiment, mesurament, anàlisi i avaluació que es fan servir, així com s'indica per part de qui i en quins intervals temporals s'han de dur a terme. Finalment, es mostra un llistat amb els indicadors existents en l'àmbit de l'SGSI de l'Organització.

14.2 Abast

La definició dels indicadors de seguretat de la informació i de la seva gestió, tal i com es troba documentat en el present document, aplica a tots els controls de seguretat de l'SGSI de l'Organització, en tant en quan aquests són d'aplicabilitat segons l'establert a Annex VII: Declaració d'Aplicabilitat. De forma concordant amb l'abast definit a la Declaració d'Aplicabilitat i, en termes més generals, a l'abast del pla director de seguretat, els processos rellevants per a la gestió d'indicadors són:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

14.3 Estructura de l’indicador

Els indicadors utilitzats per a realitzar un monitoratge de l’SGSI de l’Organització i, en concret, dels controls de seguretat implementats, han de disposar dels següents elements, segons es desprèn de [9]:

- **Nom**: Tot indicador ha de tenir associat un nom que l’identifiqui de manera única. Aquest, a més, ha de donar una certa informació sobre quin és el mesurament que es fa.

- **Descripció**: Es tracta d’una breu definició de l’indicador, on principalment s’indica l’objectiu del mateix.

- **Control (o controls) de seguretat**: Aquest camp indica quin (o quins) control de seguretat s’han de monitorar amb el present indicador.

- **Fórmula de mesurament**: En cas que la mesura es pugui realitzar de forma numèrica, es tracta de la definició de la fórmula a aplicar per a obtenir-ne el valor mesurat. En cas que la mesura sigui qualitativa, cal indicar els paràmetres de classificació.

- **Unitat de mesura**: Quina unitat de mesura defineix el valor mesurat.

- **Freqüència de mesura**: Quina és la periodicitat amb la qual s’ha de realitzar la mesura. Cal destacar que la freqüència no te perquè ser un valor inamovible, sinó que es pot adaptar en funció de les circumstàncies (e.g. durant els primers mesos després de la implantació d’un nou indicador, sovint es realitzaran mesures en intervals de temps més petits).

- **Llindar objectiu i llindar d’alarma**: Es tracta de valors prefixats que marquen, d’una banda, quin és el valor objectiu que es vol assolir i, de l’altra, quin és el valor per sota del qual (o per sobre, en funció de com estigui definit l’indicador) s’hauria de generar una alarma.

- **Responsable**: Qui és el responsable final de dur a terme el monitoratge de l’indicador.

14.4 Monitoratge dels indicadors

A l'hora de definir els indicadors que es fan servir per a monitoritzar els controls de seguretat establerts en l'SGSI de l'Organització, a més d'indicar quins controls es volen mesurar, és necessari definir els mètodes utilitzats per a fer-ho, així com la periodicitat del monitoratge i el responsable final de cada indicador.

A 14.5 es llisten tots els indicadors dels controls de seguretat definits per a l'SGSI de l'Organització. Als capítols 14.4.1 , 14.4.2 i 14.4.3 es mostren els possibles mètodes, periodicitat i responsables que poden assignar-se als indicadors.

14.4.1 Mètodes de seguiment, mesurament, anàlisi i avaluació

El monitoratge dels indicadors de seguretat de la informació consta de dues fases diferenciades:

- **Seguiment i mesurament**: és quan es recopilen evidències del control (o controls) de seguretat a què fa referència l'indicador.

- **Anàlisi i avaluació**: és quan es revisen les evidències i s'extreu un resultat en forma d'avaluació, segons està definit a la fórmula de mesurament de l'indicador.

Tot i que sovint les dues fases estan diferenciades, tant en el punt temporal en que es duen a terme com en qui és el responsable d'executar-les, no te perquè ser sempre així. Per a alguns indicadors, tant el responsable com el moment temporal pot coincidir per a les dues fases (o haver-hi poca diferència en el temps).

Els possibles mètodes de seguiment i mesurament usats dins de l'àmbit de l'SGSI de l'Organització són:

- Revisió de l'existència i data d'última actualització de documents referents a la seguretat de la informació de l'Organització.
- Mesurament del número d'incidències ocorregudes en un període de temps determinat.
- Mesurament del número de conformitats / no-conformitats ocorregudes en un període de temps determinat.
- Mesurament del número d'empleats, actius o accions que compleixen una certa condició, ja sigui en el seu valor absolut o de forma relativa a un altre valor.

Els possibles mètodes d'anàlisi i avaluació són:

- En funció de l'existència i/o actualitat de la documentació rellevant, s'avalua l'indicador de la forma predefinida.
- Recompte del número d'incidències i comparació amb els llindars definits.
- Recompte del número de conformitats / no-conformitats i comparació amb els llindars definits.
- Recompte del número d'empleats, actius, accions, i comparació amb els llindars definits.

14.4.2 Quan i qui realitza el seguiment i el mesurament

El seguiment i mesurament es poden dur a terme o bé de manera contínua o bé de forma puntual. En el primer cas, normalment es tracta de mesuraments per part d'eines de monitoratge automatitzades (e.g. recopilació de *logs*, *firewalls*, *Intrusion Detection System* o IPS, etc). El seguiment puntual, en canvi, és una activitat que es duu a terme per part d'una persona que te assignada un rol en l'àmbit de seguretat de la informació – veure Annex V: Gestió de Rols i Responsabilitats per a més detalls. En aquest darrer cas es recolliran evidències de forma periòdica, en funció de l'establert per l'indicador de seguretat corresponent.

14.4.3 Quan i qui realitza l'anàlisi i l'avaluació

A l'hora de fer l'anàlisi i avaluació segons els criteris establerts en l'indicador de seguretat corresponent, i de forma similar a la fase anterior – veure 14.4.2 – poden aquestes realitzar-se de forma automatitzada per mitjà d'alguna eina (e.g. generar una alerta en el cas que es superi un llindar predefinit), o bé ser executades per part d'una persona o grup de persones amb facultats assignades en la seguretat de la informació de l'Organització. És habitual que els indicadors de seguretat definits a l'Organització requereixin d'un o més rols de seguretat a l'hora de fer l'avaluació final i, si s'escau, prendre les decisions correctives adients.

14.5 Indicadors dels controls implementats a l'Organització

A continuació es mostren els indicadors establerts a l'SGSI de l'Organització.

Nom	Control de polítiques de seguretat
Descripció	Mesura de l'existència de polítiques de seguretat actualitzades (o revisades acceptant cap actualització)
Control (o controls) de seguretat	A.5.1.1: Polítiques per la seguretat de la informació A.5.1.2: Revisió de les polítiques per la seguretat de la informació A.6.2.1: Política de dispositius mòbils A.6.2.2: Teletreball A.9.1.1: Política de control d'accés A.10.1.1: Política d'usos dels controls criptogràfics A.13.2.1: Polítiques i procediments d'intercanvi d'informació A.13.2.2: Acords d'intercanvi d'informació A.13.2.3: Missatgeria electrònica A.13.2.4: Acords de confidencialitat o no revelació A.14.2.1: Política de desenvolupament segur A.15.1.1: Política de seguretat de la informació en les relacions amb els proveïdors
Fórmula de mesurament	N° de polítiques revisades en els últims 365 dies sobre el n° total de polítiques
Unitat de mesura	N° de polítiques revisades / n° total de polítiques
Freqüència de mesura	Trimestralment
Llindar objectiu	100%
Llindar d'alarma	< 80%
Responsable	Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat o de forma individual

Taula 50: Indicador - control de polítiques de seguretat

Nom	Validesa de l'organització interna
Descripció	Mesura de l'adequació de l'organització interna establerta i documentada
Control (o controls) de seguretat	A.6.1.1: Rols i responsabilitats en seguretat de la informació A.6.1.2: Segregació de tasques A.6.1.3: Contacte amb les autoritats A.6.1.4: Contacte amb grups d'interès especial A.6.1.5: Seguretat de la informació en la gestió de projectes
Fórmula de mesurament	Incidències o no-conformitats reportades en el període d'un mes

Nom	Validesa de l’organització interna
Unitat de mesura	Incidències o no-conformitats / 30 dies
Freqüència de mesura	Cada 6 mesos
Llindar objectiu	0 incidències o no-conformitats
Llindar d’alarma	> 5 incidències o no-conformitats
Responsable	Direcció, en l’àmbit de les reunions de revisió per direcció (Per al control A.6.1.5, la direcció s’ajudarà del suport del CISO)

Taula 51: Indicador - validesa de l’organització interna

Nom	Control d’antecedents
Descripció	Mesura del correcte control d’antecedents previ a la contractació de nous empleats
Control (o controls) de seguretat	A.7.1.1: Investigació d’antecedents
Fórmula de mesurament	Empleats no aptes per a desenvolupar les tasques un cop ja formen part de la plantilla (degut a antecedents) sobre el total d’empleats
Unitat de mesura	Empleats no aptes / Total d’empleats
Freqüència de mesura	Trimestral
Llindar objectiu	0%
Llindar d’alarma	> 0%
Responsable	Responsable de seguretat a partir d’informació de RRHH

Taula 52: Indicador - control d'antecedents

Nom	Mesura de la definició de les condicions i responsabilitats
Descripció	Mesura de la correcte definició de les condicions laborals i les responsabilitats en matèria de seguretat de la informació associades
Control (o controls) de seguretat	A.7.1.2: Condicions de treball A.7.2.1: Responsabilitats de gestió A.7.2.3: Procés disciplinari
Fórmula de mesurament	Incidències o no-conformitats, respecte a les condicions i responsabilitats acordades i transmeses al nou empleat, reportades en el període d’un mes
Unitat de mesura	Incidències o no-conformitats / 30 dies
Freqüència de mesura	Cada 6 mesos
Llindar objectiu	0 incidències o no-conformitats
Llindar d’alarma	> 5 incidències o no-conformitats

Nom	Mesura de la definició de les condicions i responsabilitats
Responsable	Direcció, en l'àmbit de les reunions de revisió per direcció (ajudat d'informació provinent de RRHH)

Taula 53: Indicador - mesura de la definició de les condicions i responsabilitats

Nom	Mesura de campanyes de conscienciació
Descripció	Mesura de la realització de campanyes de conscienciació en matèria de seguretat de la informació a l'Organització
Control (o controls) de seguretat	A.7.2.2: Conscienciació, educació i capacitació en seguretat de la informació
Fórmula de mesurament	N° de campanyes realitzades en els últims 365 dies
Unitat de mesura	N° de campanyes realitzades
Freqüència de mesura	Cada 6 mesos
Llindar objectiu	3 a l'any
Llindar d'alarma	< 2 a l'any
Responsable	Direcció i Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat o de forma individual

Taula 54: Indicador - mesura de campanyes de conscienciació

Nom	Control de l'inventari d'actius
Descripció	Inventari actualitzat dels actius de l'Organització, i si aquest compleix els requisits necessaris: - Tots els actius estan inventariats, incloent els suports extraïbles - L'actiu te un propietari - Hi ha definides normes d'ús sobre l'actiu, incloent els suports físics en trànsit - Els actius que ja no són requerits són retornats/eliminats i marcats com a tal, incloent els suports extraïbles
Control (o controls) de seguretat	A.8.1.1: Inventari d'actius A.8.1.2: Propietat dels actius A.8.1.3: Ús acceptable dels actius A.8.1.4: Devolució d'actius A.8.3.1: Gestió de suports extraïbles A.8.3.2: Eliminació de suports A.8.3.3: Suports físics en trànsit A.11.2.7: Reutilització o eliminació segura d'equips
Fórmula de mesurament	N° d'actius que presenten una no-conformitat respecte a algun dels requisits necessaris d'inventari.
Unitat de mesura	N° d'actius que presenten una no-conformitat / n° d'actius total

Nom	Control de l’inventari d’actius
Freqüència de mesura	Trimestralment
Llindar objectiu	0%
Llindar d’alarma	> 20%
Responsable	*IT Manager*, ajudant-se en el CISO per al control A.8.1.3

Taula 55: Indicador - control de l’inventari d’actius

Nom	Mesura del tipus d’informació
Descripció	Mesura del compliment d’etiquetat i manipulació de la informació, segons l’establert a la política de classificació de la informació
Control (o controls) de seguretat	A.8.2.1: Classificació de la informació A.8.2.2: Etiquetat de la informació A.8.2.3: Manipulació de la informació
Fórmula de mesurament	Incidències o no-conformitats reportades en el període d’un mes
Unitat de mesura	Incidències o no-conformitats / 30 dies
Freqüència de mesura	Trimestralment
Llindar objectiu	0 incidències o no-conformitats
Llindar d’alarma	> 2 incidències o no-conformitats
Responsable	Responsable de seguretat de la informació

Taula 56: Indicador - mesura del tipus d’informació

Nom	Control de l’accés a xarxes, servidors i serveis
Descripció	Mesura del funcionament dels controls d’accés a les diferents xarxes, servidors i serveis de l’Organització, tant si es garanteix l’accés a usuaris o entitats legítims com si se’l denega als il·legítims
Control (o controls) de seguretat	A.9.1.2: Accés a les xarxes i als servidors de xarxa A.13.1.1: Controls de xarxa A.13.1.2: Seguretat dels serveis de xarxa A.9.4.5: Control d’accés al codi font dels programes A.9.4.1: Restricció de l’accés a la informació
Fórmula de mesurament	N° d’accessos erronis (legítims denegats o il·legítims concedits) sobre el total d’intents d’accés
Unitat de mesura	N° accessos erronis / n° total intents d’accés
Freqüència de mesura	Mensual
Llindar objectiu	0%

Nom	Control de l’accés a xarxes, servidors i serveis
Llindar d’alarma	> 10%
Responsable	Responsable de seguretat de la informació, a partir de la informació proporcionada per les eines de monitoratge d’accés

Taula 57: Indicador - control de l’accés a xarxes, servidors i serveis

Nom	Control de privilegis d’accés en cas de cessament d’activitats
Descripció	Control de la retirada de privilegis als empleats o subcontractistes que ja no treballin per a l’Organització o bé que ja no necessitin privilegis d’accés per haver canviat de projectes
Control (o controls) de seguretat	A.7.3.1: Responsabilitats davant la finalització o canvi A.9.2.1: Registre i baixa d’usuari A.9.2.6: Retirada o reassignació dels drets d’accés
Fórmula de mesurament	N° de baixes i retirada de privilegis sobre el n° de cessament d’activitats en un projecte o baixes completes a l’Organització
Unitat de mesura	N° de baixes i retirada de privilegis / n° de cessament d’activitats
Freqüència de mesura	Trimestral
Llindar objectiu	100%
Llindar d’alarma	< 80%
Responsable	Responsable de seguretat de la informació, a partir de la informació proporcionada per les eines de monitoratge d’accés i d’informacions provinents de RRHH

Taula 58: Indicador - control de privilegis d’accés en cas de cessament d’activitats

Nom	Control de privilegis d’accés en cas d’incorporació d’activitats
Descripció	Control de l’assignació de privilegis als nous empleats o subcontractistes, o bé a aquells que iniciïn una nova activitat en l’àmbit d’un projecte de l’Organització
Control (o controls) de seguretat	A.9.2.2: Provisió d’accés d’usuari A.9.2.3: Gestió de privilegis d’accés A.9.4.4: Ús d’utilitats amb privilegis del sistema
Fórmula de mesurament	N° d’assignació de privilegis sobre el n° de noves altes a l’Organització o a un projecte de la mateixa
Unitat de mesura	N° d’assignació de privilegis / n° de noves altes
Freqüència de mesura	Trimestral
Llindar objectiu	100%
Llindar d’alarma	< 80%

Nom	Control de privilegis d’accés en cas d’incorporació d’activitats
Responsable	Responsable de seguretat de la informació, a partir de la informació proporcionada per les eines de monitoratge d’accés i d’informacions provinents de RRHH

Taula 59: Indicador - control de privilegis d’accés en cas d’incorporació d’activitats

Nom	Control d’inici de sessió segur
Descripció	Mesura del nivell de seguretat dels mecanismes d’inici de sessió, així com d’aquelles dades necessàries per a dur-lo a terme (credencials)
Control (o controls) de seguretat	A.9.2.4: Gestió de la informació secreta d’autenticació dels usuaris A.9.3.1: Ús de la informació secreta d’autenticació A.9.4.2: Procediments d’inici de sessió A.9.4.3: Sistema de gestió de contrasenyes A.10.1.2: Gestió de claus
Fórmula de mesurament	Incidències funcionals o de revelació de secrets reportades en el període d’un mes
Unitat de mesura	Incidències / 30 dies
Freqüència de mesura	Trimestralment
Llindar objectiu	0 incidències
Llindar d’alarma	> 2 incidències funcionals o bé > 1 incidències de revelació de secrets
Responsable	Responsable de seguretat de la informació

Taula 60: Indicador - control d’inici de sessió segur

Nom	Revisió de privilegis d’accés
Descripció	Control de l’actualitat dels privilegis d’accés existents
Control (o controls) de seguretat	A.9.2.5: Revisió dels drets d’accés d’usuari
Fórmula de mesurament	N° de privilegis d’accés revisats en els últims 365 dies sobre el n° total de privilegis existents
Unitat de mesura	N° de privilegis d’accés revisats / N° total de privilegis existents
Freqüència de mesura	Trimestralment
Llindar objectiu	100%
Llindar d’alarma	< 80%
Responsable	Responsable de seguretat de la informació, a partir de la informació proporcionada per les eines de monitoratge d’accés

Taula 61: Indicador - revisió de privilegis d’accés

Nom	Control de l’accés físic a les instal·lacions de l’Organització
Descripció	Mesura del funcionament dels controls d’accés físic a les instal·lacions de l’Organització, tant si es garanteix l’accés a usuaris o entitats legítims com si se’l denega als il·legítims
Control (o controls) de seguretat	A.11.1.1: Perímetre de seguretat física A.11.1.2: Controls físics d’entrada
Fórmula de mesurament	N° d’accessos erronis (legítims denegats o il·legítims concedits) sobre el total d’intents d’accés
Unitat de mesura	N° accessos erronis / n° total intents d’accés
Freqüència de mesura	Trimestral
Llindar objectiu	0%
Llindar d’alarma	> 10%
Responsable	Responsable de seguretat de la informació, a partir de la informació proporcionada per les eines de monitoratge d’accés

Taula 62: Indicador - control de l’accés físic a les instal·lacions de l’Organització

Nom	Mesura de la seguretat a les instal·lacions i equips
Descripció	Mesura de les incidències de seguretat en les instal·lacions de l’Organització i/o en els equips, ja es trobin aquests dins de de les instal·lacions o en una altra ubicació
Control (o controls) de	A.11.1.4: Protecció contra les amenaces externes i ambientals

Nom	Mesura de la seguretat a les instal·lacions i equips
seguretat	A.11.2.1: Emplaçament i protecció d'equips A.11.2.2: Instal·lacions de subministrament A.11.2.3: Seguretat del cablejat A.11.2.6: Seguretat dels equips fora de les instal·lacions
Fórmula de mesurament	Incidències reportades en el període d'un mes
Unitat de mesura	Incidències / 30 dies
Freqüència de mesura	Trimestralment
Llindar objectiu	0 incidències
Llindar d'alarma	> 2 incidències
Responsable	Responsable de seguretat de la informació, ajudat per l'*IT Manager*

Taula 63: Indicador - mesura de la seguretat a les instal·lacions i equips

Nom	Control del manteniment dels equips i sistemes d'informació
Descripció	Control del nivell actual de manteniment dels equips, tant en hardware com en software, així com dels sistemes d'informació
Control (o controls) de seguretat	A.11.2.4: Manteniment dels equips A.12.7.1: Controls d'auditoria de sistemes d'informació
Fórmula de mesurament	N° d'equips i sistemes revisats en els últims 6 mesos (si el hardware i el software segueixen essent actuals i vàlids) sobre el n° d'equips i sistemes total
Unitat de mesura	N° d'equips i sistemes revisats / n° d'equips i sistemes total
Freqüència de mesura	Trimestralment
Llindar objectiu	100%
Llindar d'alarma	< 80%
Responsable	*IT Manager*

Taula 64: Indicador - control del manteniment dels equips i sistemes d'informació

Nom	Control d'equip d'usuari desatès
Descripció	Observació d'equips d'usuari desatesos i plenament operatius (e.g. sense bloquejar)
Control (o controls) de seguretat	A.11.2.8: Equip d'usuari desatès
Fórmula de mesurament	N° d'equips d'usuari desatesos observats en l'últim mes
Unitat de mesura	N° d'equips d'usuari desatesos / 30 dies
Freqüència de mesura	Trimestralment

Nom	Control d’equip d’usuari desatès
Llindar objectiu	0%
Llindar d’alarma	> 10%
Responsable	Responsable de seguretat de la informació, recopilant informació de tots els treballadors

Taula 65: Indicador - control d’equip d’usuari desatès

Nom	Mesura de la documentació de procediments d’operació
Descripció	Control de l’existència i actualitat de la documentació sobre procediments i gestions operatives
Control (o controls) de seguretat	A.12.1.1: Documentació de procediments d’operació A.12.1.2: Gestió de canvis A.12.1.3: Gestió de capacitats A.14.2.2: Procediment de control de canvis en sistemes A.14.2.3: Revisió tècnica de les aplicacions després d’efectuar canvis en el sistema operatiu
Fórmula de mesurament	N° de procediments revisats i/o actualitzats en els últims 365 dies sobre el n° total de procediments
Unitat de mesura	N° de procediments revisats / n° total de procediments
Freqüència de mesura	Cada 12 mesos
Llindar objectiu	100%
Llindar d’alarma	< 80%
Responsable	Responsable de seguretat de la informació, en l’àmbit del Comitè de seguretat o de forma individual

Taula 66: Indicador - mesura de la documentació de procediments d’operació

Nom	Control del desplegament de software
Descripció	Mesura de l’existència i actualitat de normes i guies que defineixin quin software es pot instal·lar a quin entorn, quan i com
Control (o controls) de seguretat	A.12.1.4: Separació dels recursos de desenvolupament, prova i operació A.12.5.1: Instal·lació del software en explotació A.12.6.2: Restricció en la instal·lació de software A.14.2.4: Restriccions als canvis als paquets de software
Fórmula de mesurament	N° de normes i guies revisades en els últims 365 dies sobre el n° total de normes i guies
Unitat de mesura	N° de normes i guies revisades / n° total de normes i guies

Nom	Control del desplegament de software
Freqüència de mesura	Cada 12 mesos
Llindar objectiu	100%
Llindar d'alarma	< 80%
Responsable	Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat o de forma individual

Taula 67: Indicador - control del desplegament de software

Nom	Control d'incidents de seguretat
Descripció	Mesura sobre els incidents de seguretats ocorreguts en els processos de negoci de l'Organització en el període d'un mes
Control (o controls) de seguretat	A.12.2.1: Controls contra el codi maliciós A.12.6.1: Gestió de les vulnerabilitats tècniques A.14.1.2: Assegurar els serveis d'aplicacions en xarxes públiques A.14.1.3: Protecció de les transaccions de serveis d'aplicacions
Fórmula de mesurament	Incidències de seguretat reportades en el període d'un mes
Unitat de mesura	Incidències / 30 dies
Freqüència de mesura	Trimestralment
Llindar objectiu	0 incidències
Llindar d'alarma	> 2 incidències
Responsable	Responsable de seguretat de la informació

Taula 68: Indicador - control d'incidents de seguretat

Nom	Control de *backups* i redundàncies
Descripció	Mesura de la quantitat d'informació de l'Organització que està recolzada amb una còpia de seguretat o amb redundàncies d'altre tipus
Control (o controls) de seguretat	A.12.3.1: Còpies de seguretat de la informació A.17.2.1: Disponibilitat dels recursos de tractament de la informació
Fórmula de mesurament	N° d'equips redundats o de discs dels quals es manté una còpia de seguretat actual sobre el n° d'equips o discs total
Unitat de mesura	N° d'equips redundats o de discs amb *backup* / n° total d'equips o de discs
Freqüència de mesura	Mensual
Llindar objectiu	100%
Llindar d'alarma	< 90%
Responsable	*IT Manager*

Taula 69: Indicador - control de backups i redundàncies

Nom	Control de la gestió de la informació del registre d'events
Descripció	Mesura dels controls destinats a recopilar informació sobre els events que es generen dins de l'SGSI i gestionar-la de forma segura
Control (o controls) de seguretat	A.12.4.1: Registre d'events A.12.4.2: Protecció de la informació del registre A.12.4.3: Registres d'administració i operació A.12.4.4: Sincronització del rellotge
Fórmula de mesurament	Incidències o no-conformitats reportades en el període d'un mes
Unitat de mesura	Incidències o no-conformitats / 30 dies
Freqüència de mesura	Trimestralment
Llindar objectiu	0 incidències o no-conformitats
Llindar d'alarma	> 5 incidències o no-conformitats
Responsable	Responsable de seguretat de la informació

Taula 70: Indicador - control de la gestió de la informació del registre d'events

Nom	Control dels requeriments de xarxa i desenvolupament segurs
Descripció	Mesura de l'existència i actualitat de normes i guies que defineixin quin software es pot instal·lar a quin entorn, quan i com
Control (o controls) de seguretat	A.13.1.3: Segregació en xarxes A.14.1.1: Anàlisi de requisits i especificacions de seguretat de la informació A.14.2.5: Principis d'enginyeria de sistemes segurs

Nom	Control dels requeriments de xarxa i desenvolupament segurs
	A.14.2.6: Entorn de desenvolupament segur A.14.2.7: Externalització del desenvolupament de software
Fórmula de mesurament	N° de requeriments revisats en els últims 365 dies sobre el n° total de requeriments
Unitat de mesura	N° de requeriments revisats / n° total de requeriments
Freqüència de mesura	Cada 12 mesos
Llindar objectiu	100%
Llindar d'alarma	< 75%
Responsable	Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat o de forma individual

Taula 71: Indicador - control dels requeriments de xarxa i desenvolupament segurs

Nom	Control de proves
Descripció	Mesura de l'existència i actualitat de procediments que defineixin les proves a executar, com a part de les proves funcionals i d'acceptació de sistemes, i la gestió segura de les dades emprades per a les mateixes
Control (o controls) de seguretat	A.14.2.8: Proves funcionals de seguretat de sistemes A.14.2.9: Proves d'acceptació de sistemes A.14.3.1: Protecció de les dades de prova
Fórmula de mesurament	N° de procediments de prova revisats en els últims 365 dies sobre el n° total de procediments de prova
Unitat de mesura	N° de procediments de prova revisats / n° total de procediments de prova
Freqüència de mesura	Cada 12 mesos
Llindar objectiu	100%
Llindar d'alarma	< 75%
Responsable	Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat o de forma individual

Taula 72: Indicador - control de proves

Nom	Control de documentació de relació amb proveïdors
Descripció	Control de l'existència i actualitat de la documentació sobre el tracte amb proveïdors, ja sigui per a l'adquisició d'equips, software o serveis d'informació, o bé per al control i gestió de canvis
Control (o controls) de seguretat	A.15.1.2: Requisits de seguretat en contractes amb tercers A.15.1.3: Cadena de subministrament de tecnologia de la informació i de les

Nom	Control de documentació de relació amb proveïdors comunicacions A.15.2.1: Control i revisió de la provisió de serveis del proveïdor A.15.2.2: Gestió de canvis en la provisió del servei del proveïdor
Fórmula de mesurament	N° de documents revisats en els últims 365 dies sobre el n° total de documents
Unitat de mesura	N° de documents revisats / n° total de documents
Freqüència de mesura	Cada 12 mesos
Llindar objectiu	100%
Llindar d'alarma	< 75%
Responsable	Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat (necessàriament també amb la direcció, al tractar-se de contractes)

Taula 73: Indicador - control de documentació de relació amb proveïdors

Nom	Control de procediments de gestió d'incidents de seguretat
Descripció	Control de l'existència i actualitat de la documentació sobre procediments de gestió d'incidents de seguretat
Control (o controls) de seguretat	A.16.1.1: Responsabilitats i procediments A.16.1.2: Notificació dels events de seguretat de la informació A.16.1.3: Notificació de punts dèbils de la seguretat A.16.1.4: Avaluació i decisió sobre els events de seguretat de la informació A.16.1.5: Resposta a incidents de seguretat de la informació A.16.1.6: Aprenentatge dels incidents de seguretat de la informació A.16.1.7: Recopilació d'evidències
Fórmula de mesurament	N° de procediments revisats en els últims 365 dies sobre el n° total de procediments
Unitat de mesura	N° de procediments revisats / n° total de procediments
Freqüència de mesura	Cada 12 mesos
Llindar objectiu	100%
Llindar d'alarma	< 80%
Responsable	Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat

Taula 74: Indicador - control de procediments de gestió d'incidents de seguretat

Nom	Control de la continuïtat del negoci
Descripció	Mesura de l'existència i actualitat d'un pla de continuïtat del negoci en termes de seguretat de la informació, així com del grau d'implantació actual
Control (o controls) de	A.17.1.1: Planificació de la continuïtat de la seguretat de la informació

Nom	Control de la continuïtat del negoci
seguretat	A.17.1.2: Implementar la continuïtat de la seguretat de la informació A.17.1.3: Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació
Fórmula de mesurament	N° de mesures vigents/actuals i implementades completament sobre el n° total de mesures planificades
Unitat de mesura	N° de mesures vigents i implementades / n° total de mesures planificades
Freqüència de mesura	Cada 12 mesos
Llindar objectiu	100%
Llindar d'alarma	< 90%
Responsable	Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat (es requerirà la presència de l'*IT Manager*)

Taula 75: Indicador - control de la continuïtat del negoci

Nom	Compliment de la legislació aplicable
Descripció	Mesura del compliment de la legislació aplicable als processos de negoci de l'Organització, i de l'actualització en cas necessari
Control (o controls) de seguretat	A.18.1.1: Identificació de la legislació aplicable i dels requisits contractuals A.18.1.2: Drets de propietat intel·lectual (DPI) A.18.1.3: Protecció dels registres de la organització A.18.1.4: Protecció i privacitat de la informació de caràcter personal A.18.1.5: Regulació dels controls criptogràfics
Fórmula de mesurament	N° de lleis, reglaments i procediments revisats en els últims 365 dies sobre el n° total de lleis, reglaments i procediments
Unitat de mesura	N° de procediments revisats / n° total de procediments
Freqüència de mesura	Cada 6 mesos
Llindar objectiu	100%
Llindar d'alarma	< 95%
Responsable	Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat (cal avaluar-ho conjuntament amb la direcció)

Taula 76: Indicador - compliment de la legislació aplicable

Nom	Revisió de la seguretat de la informació
Descripció	Control sobre l'actualitat de les revisions o auditories de l'SGSI de l'Organització, tant de forma interna com de forma independent
Control (o controls) de	A.18.2.1: Revisió independent de la seguretat de la informació

Nom	Revisió de la seguretat de la informació
seguretat	A.18.2.2: Compliment de les polítiques i normes de seguretat A.18.2.3: Comprovació del compliment tècnic
Fórmula de mesurament	N° de requisits tècnics i organitzatius superats en l'última revisió sobre el n° total de requisits exigits en la revisió
Unitat de mesura	N° de requisits superats / n° total de requisits
Freqüència de mesura	Cada 12 mesos
Llindar objectiu	100%
Llindar d'alarma	< 75%
Responsable	Responsable de seguretat de la informació, en l'àmbit del Comitè de seguretat (cal avaluar-ho amb diversos responsables, entre d'altres, amb el responsable de qualitat de l'Organització)

Taula 77: Indicador - revisió de la seguretat de la informació

15. Annex IV: Procediment de Revisió per Direcció

Control de versions

Versió	Data	Descripció dels canvis
V1	09/03/2022	Versió inicial del document

15.1 Introducció

Tant l'SGSI com la Organització mateixa són elements dinàmics i, per tant, subjectes al canvi en el temps. Aquesta característica intrínseca dels seus processos, juntament amb la necessitat d'avaluar de manera regular la idoneïtat del sistema de gestió de la seguretat de la informació implantat, fa necessari les revisions periòdiques de l'SGSI. Aquestes revisions, i segons es defineix a la clàusula 9.3 de la norma ISO/IEC 27001 [3], s'han de dur a terme per part de la direcció de l'entitat, per ser aquesta la part de l'estructura organitzativa amb més potestat de decisió, també en matèria de seguretat de la informació.

El document de Procediment de Revisió per Direcció presenta el procediment formal que defineix les revisions regulars de l'SGSI de l'Organització. En aquest, s'hi defineixen els temes a tractar en les revisions, els participants necessaris i els opcionals, i quina és la periodicitat que cal complir.

15.2 Abast

El procediment de revisió per part de la direcció, tal i com està definit en el present document, es limita a definir les revisions de l'SGSI, el qual està dissenyat i implementat en concordança a l'abast definit al pla director de seguretat:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

15.3 Procediment de revisió per la direcció

Les revisions de l'SGSI, a més de ser un requisit per al compliment de la normativa en seguretat de la informació ISO 27001 [3], són un element fonamental per a assolir i mantenir els objectius de seguretat definits a la política de seguretat de la informació de l'Organització. L'avaluació periòdica del sistema de gestió de seguretat de la informació proporciona una visió actualitzada de l'estat actual del sistemes de seguretat, així com permet establir les bases per a la presa de decisions. Més enllà d'afectar els processos relacionats amb la seguretat de la informació, les revisions poden ajudar a detectar la necessitat de realitzar canvis o adaptacions en altres àmbits de l'Organització.

Les revisions de l'SGSI es duen a terme com a reunions, ja siguin aquestes realitzades de forma presencial dins de les instal·lacions de l'Organització, o bé de forma telemàtica, fent servir les plataformes de comunicació audiovisual habituals en altres reunions. Les reunions de revisió de l'SGSI són organitzades pel director de l'Organització o, alternativament, per part d'algun membre de l'equip directiu amb facultats de representació.

15.3.1 Participants de la revisió

Com s'indica a 15.3 , les revisions són sempre organitzades per algun membre de l'equip directiu de l'Organització, de la qual cosa es desprèn que la direcció és un dels participants necessaris de les reunions de revisió de l'SGSI. No te perquè ser, però, l'única part implicada. A continuació es mostra el conjunt de participants d'aquestes reunions:

- **Direcció**: La seva presència és imprescindible. És la part que organitza les trobades i qui, en ultima instància, prendrà les decisions que es desprenguin de la revisió.

- **Responsable de seguretat de la informació o CISO**: La seva presència no és imprescindible, sinó que està subjecte al criteri de la direcció de l'Organització. Acostuma a ser una font molt valuosa per aportar dades i coneixement respecte a l'SGSI implantat.

- **Responsable d'IT o *IT Manager***: Pot participar de les revisions, de manera puntual i a criteri de la direcció.

- **Responsables d'altres àrees**: Poden participar de les revisions, de manera puntual i a criteri de la direcció.

El conjunt de participants és semblant als rols que conformen el Comitè de seguretat, definit a Annex V: Gestió de Rols i Responsabilitats. La diferència principal recau en l'enfocament

de les reunions: en el cas de les revisions de l'SGSI es tracta de reunions més encarades a fer un seguiment regular de l'SGSI i, sobretot, a prendre decisions amb gran impacte dins de l'Organització. Aquestes reunions són, a més, sempre liderades per algun membre de la direcció. Una altra diferència és que la resta de participants són tots opcionals.

15.3.2 Agenda de la revisió

En les reunions de revisió es tractaran, com a mínim, els següents punts:

- Estat de les accions d'anteriors revisions. Si una acció es tanca en una reunió, aquesta s'esmentarà a la següent reunió i es podrà eliminar de la llista d'accions per a la subsegüent.

- Incidències o canvis en les situacions internes o externes que hagin succeït en el període entre l'última reunió de revisió i l'actual, i que siguin rellevants per a l'SGSI de l'Organització.

- Informació sobre l'estat actuat de l'SGSI de l'Organització:

    - Àrees de l'SGSI que no estan funcionant com és d'esperar (no conformitats), així com les accions correctives a emprendre.
    - Seguiment dels mesuraments que es realitzen de manera regular sobre els controls de seguretat i mitjançant els indicadors establerts.
    - Resultat de les auditories.
    - Compliment dels objectius de seguretat establerts a la política de seguretat de la informació.
    - Comentaris i feedback sobre totes les parts interessades en l'SGSI: totes les parts internes de l'Organització, així com els subcontractistes i altres terceres parts que treballen amb l'Organització.
    - Resultats de l'apreciació dels riscos, així com l'estat del pla de tractament de riscos.
    - Oportunitats de millora contínua.

És possible que s'incorporin nous punts a l'agenda, sempre que així ho sol·liciti alguna de les parts. En tot cas, la representació de la direcció de l'Organització haurà d'aprovar la inclusió del tema a l'ordre del dia.

Es documentarà de forma escrita, en forma d'actes de la reunió (el que en anglès s'anomena MoM o *Minutes of Meeting*), i per a cadascun dels temes tractats:

- Breu descripció del punt tractat.
- Antecedents i fets objectius relacionats amb el tema tractat.
- Alternatives discutides en cas que s'hagi de prendre una decisió.

- Decisió final escollida, juntament amb la persona que avala la decisió.

Hi haurà un encarregat de documentar les MoM. La persona que realitzarà aquesta tasca pot variar en cada reunió. És important, però, que s'acordi formalment a l'inici de cada revisió qui en serà l'encarregat.

15.3.3 Periodicitat

Les revisions per part de la direcció de l'Organització es duran a terme de forma periòdica, en intervals que no han de superar en cap cas els 12 mesos. Sovint aquests intervals es reduiran a la meitat (6 mesos) o menys, en funció de la necessitat actual. Per exemple, pot ser necessari realitzar revisions després de curts períodes de temps en cas de canvis substancials en el sistema de gestió de la seguretat (e.g. aplicació de mesures després d'un incident greu de seguretat), o abans o després dels processos d'auditoria, després d'altes o baixes d'empleats amb gran rellevància per l'SGSI (e.g. el CISO), etc.

16. Annex V: Gestió de Rols i Responsabilitats

Control de versions

Versió	Data	Descripció dels canvis
V1	10/03/2022	Versió inicial del document

16.1 Introducció

Un dels requisits indispensables per a garantir un nivell de protecció adequat de la informació de l'Organització – és un dels primers objectius de la política de seguretat de la informació – és disposar d'una organització clara i documentada dels rols i responsabilitats en matèria de seguretat. Aquesta és, doncs, la finalitat del present document, en el qual s'exposa quina és la organització general de seguretat, així com s'identifiquen els rols existents i les responsabilitats associades. A més, també s'introdueix la funció del Comitè de seguretat de la informació, figura indispensable a l'hora d'avaluar i prendre decisions dins d'aquest àmbit.

16.2 Abast

La definició dels rols i responsabilitats del present document aplica a totes aquelles persones que formen part de l'Organització o que hi treballen de forma conjunta, ja sigui en forma de subcontractistes o com a terceres parts, les tasques i funcions de les quals estan relacionades amb els processos de negoci de l'Organització següents, en concordança amb l'abast definit al pla director de seguretat:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

16.3 Organització de la seguretat de la informació

La seguretat de la informació juga un paper fonamental dins de l'estratègia de l'Organització, essent aquesta imprescindible per a garantir la continuïtat dels processos de negoci de la mateixa. És per aquest motiu que la seguretat de la informació queda organitzada de forma transversal dins de la companyia, implicant d'una forma o altra a tots els empleats, subcontractistes i terceres parts involucrades en els processos de l'Organització.

En la següent figura es mostra, a alt nivell, l'estructura de la seguretat de la informació dins de l'Organització:

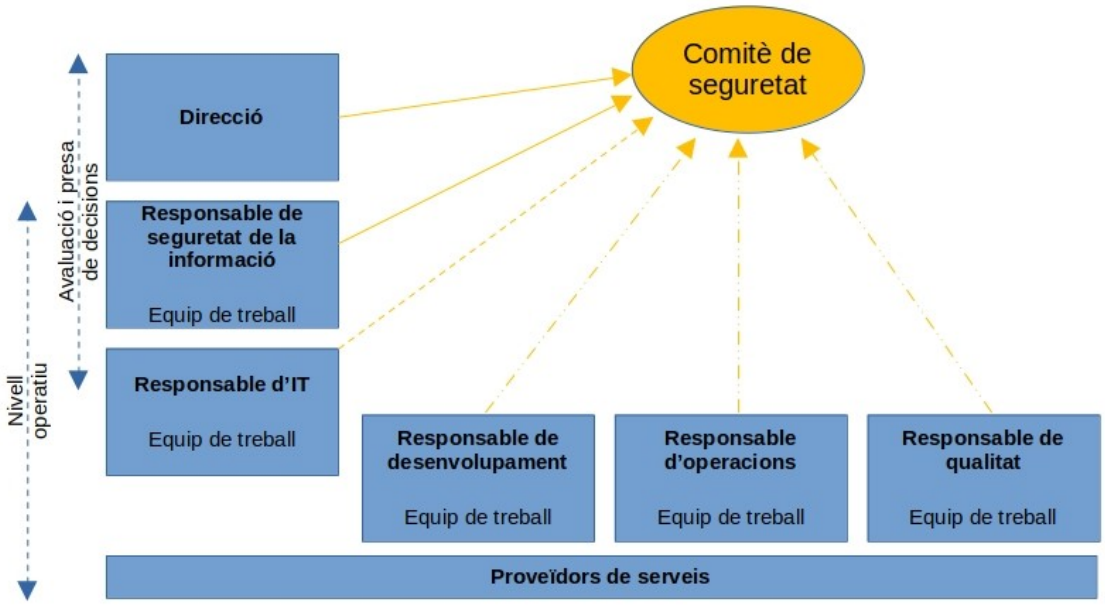


Figura 8: Organització de la seguretat de la informació

De l'anterior figura es desprèn que totes les parts involucrades en els processos de negoci de l'Organització estan implicades en la gestió de la seguretat.

D'una banda, tots els empleats, subcontractistes i terceres parts (e.g. proveïdors de serveis), han d'aplicar el que es defineix en la política de seguretat de la informació i les demés polítiques, guies i reglaments, en el seu dia a dia. Parlem aquí del nivell operatiu de la seguretat de la informació. D'altra banda, alguns rols concrets són els que realitzen preses de decisions en matèria de seguretat, prèvia avaluació de les circumstàncies que apliquin a cada cas.

Finalment, és necessari destacar l'existència del Comitè de seguretat de la informació. Aquest és un grup de treball format per diferents responsables de l'Organització – que hi participen de forma regular o bé de forma puntual – i que treballa en diferents tasques relacionades amb la seguretat de la informació.

16.3.1 Comitè de seguretat de la informació

El Comitè de seguretat de la informació està format per responsables de les diferents àrees de l'Organització, i te com a funcions principals:

- Discussió i aprovació de mesures estratègiques per a l'Organització en matèria de seguretat de la informació.
- Presa de decisions en l'àmbit de la seguretat.
- Assignació o revisió de rols en matèria de seguretat.
- Validació i aprovació del pla de riscos de l'Organització.
- Validació i aprovació de la política de seguretat de la informació i altres polítiques d'alt nivell.
- Revisió de l'estat general de l'SGSI.

Les funcions que ha de complir el Comitè de seguretat són, en gran mesura, complementàries a les que tenen els diferents rols de seguretat de la informació – veure 16.4 per a detalls sobre els rols específics existents i el conjunt de responsabilitats i tasques assignades. D'altra banda, cal destacar que algunes de les tasques del Comitè de seguretat són tractades també en les revisions de l'SGSI organitzades per la direcció de l'Organització – veure el procediment definit a Annex IV: Procediment de Revisió per Direcció.

Els membres que componen aquest grup de treball són:

- **Direcció**: Hi ha un o més membres de l'equip de direcció, ja sigui el director de l'Organització o una persona amb facultats de representació. La seva presència és imprescindible a l'hora de prendre decisions que puguin afectar als objectius estratègics de l'Organització.

- **Responsable de seguretat de la informació o CISO**: La seva presència és també imprescindible, com a persona dins de l'Organització amb la màxima autoritat en matèria de seguretat de la informació, juntament amb la direcció.

- **Responsable d'IT o *IT Manager***: És habitual que l'*IT Manager* participi de les reunions del Comitè de seguretat, degut a que sovint els actius d'IT juguen un paper fonamental en les qüestions que s'hi tracten. La seva presència no és un requisit indispensable.

- **Responsables d’altres àrees**: En funció del tema a tractar, el Comitè pot decidir la participació d’altres responsables d’àrees de l’Organització. La seva presència no és un requisit indispensable.

El Comitè de seguretat es reuneix de forma regular, en intervals que no han de superar els 6 mesos. En cas necessari, és possible convocar una reunió del Comitè de manera puntual (i, si cal, de manera urgent). Algunes situacions que habitualment requereixen d’una reunió del Comitè de seguretat fora dels terminis preestablerts són e.g. la necessitat d’avaluar mesures que afecten a l’estratègia de l’Organització, o bé si cal decidir sobre un procès de tractament d'excepcions de la política de seguretat.

16.4 Rols i responsabilitats

Es defineixen els següents rols i responsabilitats associades en l'àmbit de la seguretat de la informació de l'Organització. Degut a la naturalesa internacional de l'Organització, els rols tenen associada també una nomenclatura internacional, en anglès.

16.4.1 Cap de seguretat o *Chief information security officer* (CISO)

S'anomenarà un cap de seguretat del centre de l'Organització, al qual se li assignaran les següents funcions:

- Manteniment i actualització de la present política de seguretat de la informació.
- Disseny, redacció i manteniment de les diverses polítiques necessàries per assegurar els processos de l'Organització, emparades i en conformitat a la present política.
- Disseny, redacció i manteniment de normes i guies generals de seguretat.
- Coordinació de material i sessions de formació, per a totes les parts interessades, respecte a la seguretat de la informació a l'Organització.
- Comunicació periòdica de la política de seguretat de la informació i altres polítiques pertinents, conjuntament amb la direcció de l'Organització.
- Organització i coordinació de les mesures i controls de seguretat a implementar.
- Documentació dels diferents accessos a la informació de l'Organització, tant interns com externs.
- Mesurament i control del compliment dels objectius de seguretat de la informació.
- Representació dels interessos de la Organització en cercles de seguretat a nivell estatal i internacional.
- Realització de reunions periòdiques (mínim cada 6 mesos) amb la direcció de l'Organització per a reportar i discutir qüestions relatives a la seguretat de la informació.
- Realització de reunions periòdiques (mínim cada 6 mesos) amb l'*IT Manager* per a discutir qüestions relatives a la seguretat de la informació.
- Coordinació de les mesures a adoptar en cas d'incidents de seguretat.

16.4.2 Cap del departament de les tecnologies d'informació o *IT Manager*

Es tracta de la persona responsable del departament d'IT (de l'anglès *Information Technology*). Aquest rol te associades les següents responsabilitats, en el marc de la seguretat de la informació:

- Coordinació dels processos generals del departament d'IT.
- Avaluació de de la rendibilitat de l'aplicació de mesures en IT (anàlisi de cost-benefici).
- Disseny i implementació de projectes en l'àmbit d'IT, considerant les polítiques, normes i guies generals de seguretat establertes.
- Disseny i control dels control d'accés als diferents actius d'IT de l'Organització.
- Avaluació de l'adequació de nou hardware i software dins de la infraestructura d'IT existent.
- Coordinació de les relacions amb proveïdors de serveis d'IT, incloent l'aprovisionament de hardware i software.
- Documentació de l'estat dels actius d'IT, incloent un diagrama de xarxa actualitzat.
- Manteniment dels actius d'IT, considerant els requisits de seguretat establerts.
- Generació d'informes i dades de mesurament dels diferents controls, tal i com han estat definides conjuntament amb el CISO.
- Realització de reunions periòdiques (mínim cada 6 mesos) amb el CISO per a discutir qüestions relatives a la seguretat de la informació.

16.4.3 El proveïdor de servei o *Service provider*

El proveïdor de serveis, en tant en quant està involucrat en els processos de l'Organització, te també responsabilitats de seguretat, les quals han d'estar definides en els contractes bilaterals entre el proveïdor i l'Organització. Aquestes responsabilitat són:

- Disseny, redacció i manteniment de les diverses polítiques necessàries per assegurar els processos de l'Organització, emparades i en conformitat a la present política, sempre que aquesta sigui una de les finalitats contractuals.
- Disseny, redacció i manteniment de normes i guies generals de seguretat, sempre que aquesta sigui una de les finalitats contractuals.
- Implementació dels controls de seguretat, tal i com han estat definits pel CISO.
- Avaluació i realització d'auditories, en el cas que es tracti d'un consultor de seguretat expert en normativa ISO/IEC.
- Lectura de la política de seguretat de la informació, així com altres polítiques, que hagin estat considerades pertinents per part de la direcció de l'Organització i del responsable de seguretat.
- Compliment de les normes i regles establertes en matèria de seguretat de la informació.

16.4.4 Director del centre de l'Organització

La direcció de l'Organització, encapçalada formalment per la figura del director, te les següents responsabilitats en l'àmbit de la seguretat de la informació:

- Control del compliment dels objectius de seguretat de la informació. Aquesta tasca és delegada al rol de cap de seguretat. La responsabilitat final, però, continua residint en el rol de director.
- Nomenament dels rols de cap de seguretat i d'*IT Manager,* havent avaluat prèviament les competències de les persones candidates a ocupar-los.
- Nomenament de l'equip de treball del cap de seguretat i l'*IT Manager* (recursos personals).
- Assignació de partides pressupostàries de forma directa al cap de seguretat i l'*IT Manager*.
- Realització de reunions periòdiques (mínim cada 6 mesos) amb el responsable de seguretat per a informar-se activament sobre qüestions relatives a la seguretat de la informació. Involucrar a l'*IT Manager* en cas necessari.
- Presa de decisions quan així ho requereixi la situació i aconsellat pels experts pertinents. Sovint, en matèria de seguretat de la informació, aquests consellers seran el CISO i l'*IT Manager*.
- Avaluació i aprovació formal de la política de seguretat de la informació.
- Comunicació periòdica de la política de seguretat de la informació i altres polítiques pertinents, a tota l'Organització i parts interessades, conjuntament amb el CISO.

16.4.5 Treballadors

Tots els treballadors de l'Organització, així com els subcontractistes, tindran les següents obligacions i responsabilitats en quant a la seguretat de la informació:

- Lectura de la política de seguretat de la informació, així com altres polítiques, que hagin estat considerades pertinents per part de la direcció de l'Organització i del responsable de seguretat.
- Compliment de les normes i regles establertes en matèria de seguretat de la informació.
- Reportar sense dilació al responsable de seguretat en cas que s'observin indicis sobre un incident de seguretat o una desatenció de les normes per part de tercers que puguin desembocar en un incident.

17. Annex VI: Metodologia d'Anàlisi de Riscos

Control de versions

Versió	Data	Descripció dels canvis
V1	17/03/2022	Versió inicial del document

17.1 Introducció

L'anàlisi de riscos és un dels elements principals del pla director de seguretat de l'Organització, mitjançant el qual es busca identificar els riscos associats als actius de la mateixa, i donades una serie de possibles amenaces. Aquests riscos, que podrien afectar negativament els processos de negoci de l'Organització, cal que siguin analitzats per a, posteriorment, realitzar-ne la gestió que es consideri adequada. L'anàlisi de riscos és, a més, un requisit imprescindible per a ser conforme amb la norma internacional ISO/IEC 27001 [3]. De fet, aquest anàlisi acostuma a ser el punt de partida de tot el procés de certificació, tal i com s'esmenta a [8].

El present document defineix quina és la metodologia d'anàlisi de riscos escollida en l'àmbit de l'SGSI de l'Organització, així com n'especifica les diferents fases a dur a terme per a realitzar l'anàlisi.

17.2 Abast

L’abast del present document es focalitza en la determinació de la metodologia i passos a seguir a l’hora d’analitzar el risc en els actius involucrats en els processos de negoci de l’Organització. Com a tal, i en concordança amb l’abast determinat al pla director de seguretat, aquest es centra en els processos definits al pla director de seguretat:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

En quant a l’abast de l’anàlisi de riscos que es realitzi, aquest podrà ser definit de manera independent per a cada anàlisi. Sovint, i en cas que no s’especifiqui el contrari, l’abast dels actius a analitzar coincidirà amb el del present document i el del pla director de seguretat.

17.3 Metodologia d'anàlisi de riscos de l'Organització

La norma internacional ISO/IEC 27001, en les seves clàusules 6.1.1, 6.1.2 i 6.1.3, esmenta i justifica la necessitat de dur a terme un anàlisi de riscos de seguretat en el si d'un SGSI. Els objectius principals del tractament de riscos que es desprenen de la norma ISO 27001 [3] són:

- Garantir que l'SGSI sigui capaç d'aconseguir els resultats i objectius previstos.
- Prevenir o reduir efectes indesitjats.
- Aconseguir un procés de millora continua de l'SGSI.

Amb la finalitat d'assolir aquests objectius, els capítols següents documenten quina és la metodologia escollida per a l'SGSI de l'Organització (veure 17.3.1), així com les diverses fases que s'han de realitzar per a dur a terme l'anàlisi de riscos (veure 17.3.2 , 17.3.3 , 17.3.4 , 17.3.5 i 17.3.6).

17.3.1 Metodologia escollida: Magerit

De les diverses metodologies d'anàlisi de riscos existents, l'Organització s'ha decidit per basar-ne l'anàlisi en la metodologia Magerit. Aquesta metodologia, de forma anàloga a com ho fan la resta de metodologies que hi ha al mercat, se centra en l'anàlisi dels actius d'una organització, així com de les amenaces, vulnerabilitats i impactes potencials.

Una de les principals característiques de la metodologia Magerit, i motiu principal pel qual s'ha escollit per part de l'Organització, és que el resultat de l'anàlisi està expressat en valors econòmics/numèrics, fet que, d'una banda, complica el procediment d'aplicació de la mateixa – al requerir una conversió monetària/numèrica dels criteris tècnics – però, d'altra banda, facilita molt l'avaluació dels resultats obtinguts i la interpretació directa per part de la direcció de l'Organització. Això és així, ja que sovint hi ha una relació directe entre els valors econòmics/numèrics obtinguts i el què això significa per als processos de negoci de l'Organització. Un altre motiu per a l'elecció de Magerit com a metodologia és l'àmplia documentació existent – veure els llibres Magerit [12], [13] i [14].

17.3.2 Fase prèvia: Definició d'abast i establiment de paràmetres

Un pas previ que cal considerar a l'hora d'encarar l'anàlisi de riscos és definir quin serà l'abast del mateix, és a dir, quin conjunt de processos de l'Organització i, en conseqüència, els actius que d'una manera o altra hi estan relacionats, formaran part de l'anàlisi. En el cas de l'SGSI de l'Organització, i sempre que no s'indiqui el contrari en aquest apartat de

l’anàlisi de riscos que es dugui a terme, l’abast de l’anàlisi coincidirà amb l’abast general definit al pla director de seguretat de l’Organització. És a dir, s’identificaran i avaluaran els riscos intrínsecs als actius que participen en la preparació i posada en pràctica dels següents processos de negoci:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

En quant a l’establiment de paràmetres, cal definir prèviament a l’inici de l'anàlisi de riscos quins són els possibles valors dels següents elements:

- Valor dels actius.
- Degradació de l’actiu en cas d’afectació d’una amenaça, o impacte.
- Freqüència d'ocurrència de les amenaces, o vulnerabilitat.
- Efectivitat del control de seguretat.

En els següents capítols s’indica com queden definits els anteriors paràmetres.

17.3.3 Fase 1: Inventari i valoració d’actius

El primer que cal realitzar en aquesta fase de l’anàlisi de riscos, segons la metodologia Magerit, és identificar tots aquells actius de l’Organització que estan vinculats als processos de negoci inclosos a l’abast de l’anàlisi. A més, s’assignarà un propietari a cadascun dels actius, segons marca el control A.8.1.2 de l’ISO/IEC 27002 [1]. Un cop definits quins són els actius rellevants, aquests s’han de classificar en funció de la categoria a la qual pertanyen. Les possibles categories (o àmbits), segons la metodologia Magerit, són:

- Instal·lacions
- Hardware
- Aplicacions
- Dades
- Xarxa
- Serveis
- Equipament auxiliar
- Personal

Un cop els actius rellevants han estat identificats i categoritzats, també serà necessari definir quines interrelacions existeixen entre ells. Sovint es dona la situació que un actiu depèn directament d’un altre. Parlem, en el cas del primer actiu, de l’actiu «superior». El segon actiu, del qual depèn el primer, l’anomenem actiu «inferior». Com a part d’aquesta fase de l’anàlisi de riscos cal, doncs, definir l’arbre de dependències entre els actius.

A més de definir les categories i les relacions dels actius, és necessari analitzar-los des del punt de vista del valor que tenen dins de l'Organització. Abans de poder assignar als actius un valor o un altre, cal haver definit quines possibilitats existeixen, de manera que aquest sigui comparable entre ells. Segons el que s'indica al llibre III de Magerit [14], els possibles valors que es consideraran són:

- MA: Molt Alt
- A: Alt
- M: Mig
- B: Baix
- MB: Molt baix

A més, per a les diferents dimensions de la seguretat de la informació que es tindran en compte – veure més endavant en aquest mateix capítol –, s'assignaran valors numèrics, tal i com es mostra a la següent taula:

Valor	Criteri
10	Dany molt greu a l'Organització
7-9	Dany greu a l'Organització
4-6	Dany important a l'Organització
1-3	Dany menor a l'Organització
0	Dany irrellevant a l'Organització

Taula 78: Valoració de les dimensions de seguretat

Arribats a aquest punt, sabem quins possibles valors es poden assignar als actius identificats. Ara cal, però, saber en base a què s'han de valorar. Amb aquesta finalitat, es defineixen dos criteris fonamentals:

- **Dimensions de la seguretat de la informació** afectades, i en quina mesura. Parlem de les dimensions tradicionals de **confidencialitat**, **integritat** i **disponibilitat**(*). De forma addicional, també es consideraran les dimensions d'**autenticitat** i **traçabilitat**. La valoració de les 5 dimensions de la seguretat de la informació és el que s'anomena **valoració ACIDT**, per les seves inicials: Autenticitat, Confidencialitat, Integritat, Disponibilitat i Traçabilitat.

- Quina posició ocupa l'actiu dins de l'**arbre de dependències** entre actius. Aquesta definició de dependències es considerarà en la fase d'anàlisi d'amenaces, de manera que al tractar els actius «superiors» s'haurà d'incloure la valoració feta pels actius

«inferiors» dels primers. Per exemple, si un actiu «inferior» falla i ja no està disponible, els actius «superiors» que en depenguin tampoc ho estaran.

(*) En el cas de la dimensió de la disponibilitat, és necessari considerar com varia l'afectació d'una interrupció de la mateixa als processos de l'Organització, en funció de la durada.

Es defineixen una sèrie de preguntes a la metodologia Magerit, les quals faciliten la valoració dels actius amb els criteris esmentats anteriorment. Es poden consultar les referències al llibre I de Magerit [12], capítol 3.1.1, i al llibre II de Magerit [13], capítol 3.

Finalment, un cop identificats i categoritzats els actius, definides les seves relacions i conegudes les característiques a avaluar i amb quins possibles valors, s'haurà d'omplir una taula resum de valoració. A continuació es mostra un exemple de dita taula:

Àmbit	Actiu	Valor	Aspectes crítics				
			A	C	I	D	T
Instal·lacions	Actiu XXX	MA	6	10	8	7	6
Xarxa	Actiu XXX	MA	7	7	10	8	6
Xarxa	Actiu XXX	A	5	6	3	8	6
Serveis	Actiu XXX	M	1	2	5	2	8

Taula 79: Valoració dels actius

17.3.4 Fase 2: Anàlisi d'amenaces, impactes i vulnerabilitats

En aquesta fase de l'anàlisi de riscos, es tracta de determinar les amenaces que poden afectar de manera negativa a cadascun dels actius identificats a la fase anterior. La documentació de la metodologia Magerit proporciona un llistat d'amenaces comuns – veure [13] al capítol 5 –, les quals es faran servir per a analitzar-ne l'afectació per a cadascun dels actius de l'Organització que s'inclouen a l'abast del present anàlisi de riscos. A mode informatiu, les categories en que es classifiquen les amenaces segons Magerit són:

- Desastres naturals
- D'origen industrial
- Errors i fallides no intencionats
- Atacs intencionats

El següent pas d'aquesta fase consisteix en avaluar i documentar, per a cada amenaça i cada actiu, quin és l'impacte i la probabilitat d'ocurrència:

- **Impacte o degradació**: És el nivell de degradació del valor de l'actiu, expressat percentatge, en el cas que l'amenaça arribi a afectar l'actiu.

- **Vulnerabilitat o probabilitat**: És la probabilitat d'ocurrència de l'amenaça sobre l'actiu.

De forma similar a com es definien a 17.3.3 els possibles valors dels actius, en aquest cas cal definir quins són els possibles valors d'impacte i de vulnerabilitat.

L'impacte prendrà podrà prendre valors entre 1% i 100% (o cap valor, en cas de cap impacte negatiu), en funció de en quina fracció el valor de l'actiu queda degradat degut a la materialització d'una amenaça.

En el cas de la vulnerabilitat o probabilitat d'ocurrència, es prendrà com a mesura el número d'ocurrències a l'any (el que en anglès es denomina *Annual Rate of Occurrence* o ARO). Magerit en fa una interpretació qualitativa, que no coincideix exactament amb la definició del número de dies a l'any. S'expressa el significat en la següent taula:

100	Molt freqüent	A diari
10	Freqüent	Mensualment
1	Normal	Un cop a l'any
1/10	Poc freqüent	Cada varis anys
0	Mai	Mai

Taula 80: Vulnerabilitat o probabilitat d'ocurrència

Un cop definides les mesures de l'impacte i la vulnerabilitat, es realitzarà una taula com la que es mostra a continuació, per a cadascun dels actius identificats a 17.3.3 , i on s'indicarà quina probabilitat o freqüència d'ocurrència (vulnerabilitat) te cada amenaça sobre l'actiu, i quin impacte en cas de materialització sobre cadascuna de les dimensions de seguretat.

Amenaça	Vulnerabilitat o freqüència	A	C	I	D	T
Amenaça XXX	0	100%	50%	100%	50%	100%
Amenaça XXX	10	10%	50%	10%		50%
Amenaça XXX	1	100%	100%	100%	50%	100%
Amenaça XXX	100			1%		

Taula 81: Amenaces sobre un actiu

17.3.5 Fase 3: Determinació de l'impacte potencial

La tercera fase de l'anàlisi de riscos consisteix en calcular l'impacte potencial que tindria sobre l'Organització la materialització d'una o més amenaces. Un cop tenim definides la taula 79 (es coneix el valor dels actius) i la taula 81 (es coneix la freqüència i impacte de cada amenaça sobre cada actiu, i en aquest, sobre cada dimensió), podem calcular, per a cada amenaça – suposant que aquesta es materialitzi – quin seria l'impacte potencial per al conjunt de l'Organització. Per a determinar l'impacte potencial d'una amenaça cal:

1. Per a cada actiu, calcular l'impacte total com a la suma de les degradacions en els diferents aspectes ACIDT, i respecte als valors de l'actiu. És a dir, com a més valor inicial de l'actiu, més impacte.
2. Considerar els actius «superiors» que, tot i no veure's afectat directament per l'amenaça, es veuen degradats en el cas que l'actiu «inferior» en el que se sustenten sí estigui afectat. També és doncs necessari calcular l'impacte d'aquests actius.
3. Agregar els impactes per a cada actiu afectat per l'amenaça, ja sigui de forma directa o indirecte.

17.3.6 Fase 4: Nivell de risc acceptable i risc residual

En aquesta fase de la metodologia d'anàlisi de riscos s'aborden dos aspectes diferenciats. Abans d'especificar-los, però, cal esmentar que ambdós tenen a veure amb el risc, entès com la mesura del dany probable sobre els actius (agregats) de l'Organització. El risc, doncs, es calcula considerant el valor d'impacte potencial determinat a 17.3.5 i afegint-hi la probabilitat que aquest impacte afecti negativament a l'Organització o, el que és el mateix, la probabilitat o freqüència (o vulnerabilitat) que l'amenaça en qüestió es materialitzi. Aquest risc, ara determinat, és el que s'anomena risc potencial.

Un cop quantificat quin és el risc potencial de les amenaces en el context dels sistemes de l'Organització, es poden definir els següents dos aspectes:

- **Nivell de risc acceptable**: Es tracta de determinar el llindar del risc que delimita quin és el risc que podem assumir. Per a nivells de risc inferiors a aquest llindar, no caldrà dur a terme cap acció. Per a nivells superiors, en canvi, serà necessari aplicar controls per a reduir-lo. És important destacar que aquests llindars de risc s'han d'establir conjuntament amb la direcció de l'Organització.

- **Risc residual**: S'entén com a risc residual aquell risc que segueix existint després d'aplicar els controls de seguretat destinats a disminuir el risc potencial.

18. Annex VII: Declaració d'Aplicabilitat

Control de versions

Versió	Data	Descripció dels canvis
V1	11/03/2022	Versió inicial del document

18.1 Introducció

A l'hora d'analitzar i planificar l'establiment del SGSI de l'Organització, un dels passos imprescindibles és seleccionar quins controls de seguretat s'implementaran, els quals serviran com a mesures per a gestionar els riscos i complir els objectius de seguretat fixats a la política de seguretat de la informació. En el present document es realitza un anàlisi dels controls de seguretats proposats per l'ISO/IEC 27002 [1] i es mostra si aquests són d'aplicabilitat en el context dels processos de negoci de l'Organització.

18.2 Abast

El present document te com a objectiu definir si els diferents controls proposats per l'ISO/IEC 27002 [1] han de ser aplicats dins de l'Organització. La idoneïtat dels controls és mesurada en funció dels processos als que fa referència l'abast del pla director de seguretat:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

18.3 Declaració d’aplicabilitat

En la següent taula es mostren tots els controls definits a la ISO/IEC 27002 [1], així com la valoració de la seva aplicabilitat als processos de negoci de l’Organització. A més, també s’inclou una justificació sobre de la decisió d’incloure’ls o no.

Control	Aplica	Justificació
A.5: Polítiques de seguretat de la informació		
A.5.1: Directrius de gestió de la seguretat de la informació		
A.5.1.1: Polítiques per la seguretat de la informació	Sí	És imprescindible disposar de polítiques de seguretat que marquin els objectius a complir a nivell global. Aquestes, a més, s’han de donar a conèixer a tota l’Organització.
A.5.1.2: Revisió de les polítiques per la seguretat de la informació	Sí	Les polítiques definides i publicades, a més, han d’ésser revisades periòdicament i, en cas necessari, adaptades a les noves circumstàncies de l’Organització.
A.6: Organització de la seguretat de la informació		
A.6.1: Organització interna		
A.6.1.1: Rols i responsabilitats en seguretat de la informació	Sí	És necessari definir diferents rols, als quals cal associar-lis diferents activitats i responsabilitats. Només així és possible tractar la seguretat de la informació des de diverses perspectives i aconseguir assolir-ne els objectius de la manera més completa possible.
A.6.1.2: Segregació de tasques	Sí	Relacionat amb el control anterior, cada rol ha de tenir associades unes tasques en concret. Per tant, hi ha una segregació del conjunt total de tasques a realitzar.
A.6.1.3: Contacte amb les autoritats	Sí	Aquest control és necessari per a aquelles situacions en les quals cal contactar a les autoritats pertinents. Aquestes situacions poden ser d’índole molt diversa, e.g. un accés il·legítim a dades personals, el cas d’un incendi a la seu física, etc.
A.6.1.4: Contacte amb grups d’interès especial	Sí	De forma similar a com cal informar a les autoritats competents, a vegades també és necessari compartir la informació de seguretat rellevant amb altres grups d’interès. D’altra

Control	Aplica	Justificació
		banda, per part de l'Organització, cal mantenir-se informat d'events de seguretat que puguin ocórrer al nostre àmbit.
A.6.1.5: Seguretat de la informació en la gestió de projectes	Sí	Sabem que moltes de les activitats de l'Organització està basada en projectes i, per a que en aquests es contempli la seguretat de la informació de manera intrínseca, cal establir procediments que assegurin que aquesta es considera, e.g. amb el concepte de *Security by Design*.
A.6.2: Els dispositius mòbils i el teletreball		
A.6.2.1: Política de dispositius mòbils	Sí	L'existència i ús de dispositius mòbils fa que sigui necessari l'establiment i publicació d'una política que en reguli el seu ús en matèria de seguretat de la informació.
A.6.2.2: Teletreball	Sí	El teletreball és possible en algunes de les activitats de l'Organització, incrementat a més degut a les circumstàncies de la pandèmia en els darrers dos anys. Aquest motiu fa que calgui establir controls per a regular-ne l'ús i l'accés remot.
A.7: Seguretat relativa als recursos humans		
A.7.1: Abans del treball		
A.7.1.1: Investigació d'antecedents	Sí	Esbrinar quins són els antecedents penals d'un potencial empleat sol ser una mesura a duu a terme. En el cas de l'Organització, aquesta és a més d'obligat compliment legal, degut a algunes de les dades existents en alguns dels estudis tractats.
A.7.1.2: Condicions de treball	Sí	En les condicions laborals que s'han d'assumir per totes les parts (Organització, empleats, contractistes) hi hauria d'haver clàusules respecte a la seguretat de la informació, a mode d'evitar qualsevol tipus d'ambigüitat en casos de disputa o, simplement, per a proporcionar transparència a l'hora de transmetre les condicions.
A.7.2: Durant el treball		
A.7.2.1: Responsabilitats de gestió	Sí	És necessari que les responsabilitats en matèria de seguretat siguin recordades per part de l'Organització a totes les parts (empleats, contractistes, tercers), a més de controlar que

Control	Aplica	Justificació
		així sigui.
A.7.2.2: Conscienciació, educació i capacitació en seguretat de la informació	Sí	Amb la finalitat de millorar el compliment dels processos relacionats amb la seguretat de la informació, convé realitzar campanyes de conscienciació i educació en la temàtica.
A.7.2.3: Procés disciplinari	Sí	És necessari que existeixin processos definits per a poder prendre mesures correctives, sempre dins de l'àmbit regulatiu i legal, en cas que algunes de les accions o omissions per part d'alguna de les parts així ho requereixi.
A.7.3: Finalització del treball o canvi de lloc de treball		
A.7.3.1: Responsabilitats davant la finalització o canvi	Sí	Degut a la naturalesa de l'Organització, és habitual que hi hagi altes i baixes, tant en els empleats com en els contractistes. En el cas de baixes, s'ha de garantir que es prenen les mesures adequades, e.g. revocació de permisos.
A.8: Gestió d'actius		
A.8.1: Responsabilitat sobre els actius		
A.8.1.1: Inventari d'actius	Sí	L'Organització disposa de multitud d'actius de diferent tipus. És necessari, doncs, mantenir un inventari dels mateixos, de manera que es puguin gestionar durant tot el seu cicle de vida.
A.8.1.2: Propietat dels actius	Sí	És necessari que existeixi un propietari (o responsable) de cadascun dels actius, que serà qui vetlli pel seu manteniment, localització, etc.
A.8.1.3: Ús acceptable dels actius	Sí	Dins de totes les utilitats que se'ls hi pot donar als diferents actius, és necessari que l'Organització en defineixi aquelles que són legítimes i necessàries pel desenvolupament dels processos de negoci.
A.8.1.4: Devolució d'actius	Sí	Cal que hi hagi procediments clars i inequívocs sobre com s'han de retornar els actius en cas que ja no siguin necessaris, e.g. en cas de baixa d'un empleat o contractista.
A.8.2: Classificació de la informació		
A.8.2.1: Classificació de la informació	Sí	Existeixen diferents tipus d'informació dins de l'Organització, els quals es poden categoritzar de diferent manera (e.g. confidencial, públic, personal, etc). Per aquest motiu, és necessari que existeixin procediments per a classificar la informació.

Control	Aplica	Justificació
A.8.2.2: Etiquetat de la informació	Sí	Si existeixen diferents categories d'informació, també haurem de marcar a cadascuna d'elles amb la categoria(es) a la que pertany.
A.8.2.3: Manipulació de la informació	Sí	En funció de la categoria d'informació, aquesta s'haurà de tractar d'una manera o una altre. Aquestes normes i pautes han de quedar reflectides en procediments de manipulació de la informació.
A.8.3: Manipulació dels suports		
A.8.3.1: Gestió de suports extraïbles	Sí	Aquest control sí que és d'aplicació degut a l'existència de suports físics dins d'alguns processos de negoci de l'Organització. Aquests, doncs, s'han de gestionar d'acord a procediments establerts.
A.8.3.2: Eliminació de suports	Sí	A vegades és necessari desfer-se d'alguns suports (e.g. al fi de la seva vida útil, o al reemplaçar-los per d'altres més moderns). Per a aquests casos, també cal la redacció i publicació de procediments.
A.8.3.3: Suports físics en trànsit	Sí	Tot i que es dona en poques situacions, a vegades cal enviar suports físics dins de departaments de l'Organització, o inclús a terceres entitats. Necessitem, també en aquest cas, que hi hagi controls al respecte.
A.9: Control d'accés		
A.9.1: Requisits de negoci pel control d'accés		
A.9.1.1: Política de control d'accés	Sí	És imprescindible disposar d'una política que descrigui com s'ha de controlar l'accés a recursos i actius de l'Organització, en aquest cas posant-hi èmfasi per motius de seguretat de la informació.
A.9.1.2: Accés a les xarxes i als servidors de xarxa	Sí	L'accés a les diferents xarxes i servidors de l'Organització ha d'estar definit, controlar i monitoritzat. Recordem que existeix informació considerada confidencial, alhora que els processos de negoci (o d'estudi) depenen del bon funcionament d'aquests actius.
A.9.2: Gestió d'accés d'usuari		
A.9.2.1: Registre i baixa d'usuari	Sí	De manera similar al control A.7.3.1, és necessari gestionar de forma procedimentada les baixes d'usuaris, ja siguin empleats, contractistes o terceres parts, quan aquest accés ja no sigui

Control	Aplica	Justificació
		requerit.
A.9.2.2: Provisió d'accés d'usuari	Sí	De forma complementària al control anterior, és necessari que hi hagi procediments per a gestionar l'alta o extensió de permisos d'accés als usuaris.
A.9.2.3: Gestió de privilegis d'accés	Sí	Els privilegis d'accés s'han de gestionar sempre procurant assignar el necessari, i no més. És el que en anglès es coneix com a p*rinciple of least privilege*. És evident que, així, reduïm les possibilitats que es duguin a terme accessos no desitjats (o no dissenyats).
A.9.2.4: Gestió de la informació secreta d'autenticació dels usuaris	Sí	Ha de quedar procedimentat de forma clara, inequívoca i senzilla la forma de controlar l'accés a la informació secreta (o confidencial).
A.9.2.5: Revisió dels drets d'accés d'usuari	Sí	Els drets d'accés existents, per a un actiu en concret i un usuari en concret, han d'ésser revisats de forma periòdica, ja que les circumstàncies poden haver canviat.
A.9.2.6: Retirada o reassignació dels drets d'accés	Sí	De forma similar al control A.9.2.1, però ampliat a més supòsits (e.g. un empleat canvia d'equip o de rol), cal que existeixin procediments per a reorganitzar els drets d'accés segons correspongui.
A.9.3: Responsabilitats de l'usuari		
A.9.3.1: Ús de la informació secreta d'autenticació	Sí	Cal que la informació necessària per accedir a recursos (e.g. contrasenyes o certificats SSL) estigui gestionada de forma segura. Amb aquesta finalitat, és necessari establir procediments sobre el seu ús i gestió.
A.9.4: Control d'accés a sistemes i aplicacions		
A.9.4.1: Restricció de l'accés a la informació	Sí	D'igual manera que amb l'accés als actius – controls A.9.2.1 a A.9.2.6 – és necessari també controlar i restringir l'accés a la informació.
A.9.4.2: Procediments d'inici de sessió	Sí	Per a poder garantir una autenticació controlada, cal establir procediments d'inici de sessió segurs. Això, a més, ajudarà a l'Organització a complir l'autorització posterior.
A.9.4.3: Sistema de gestió de contrasenyes	Sí	És necessari que hi hagi uns processos definits sobre com dur a terme la gestió de contrasenyes de forma segura. Com a exemples: fer servir un gestor de contrasenyes i fixar uns requisits mínims de seguretat per a les mateixes.

Control	Aplica	Justificació
A.9.4.4: Ús d'utilitats amb privilegis del sistema	Sí	Degut al fet que sovint és necessari que més d'un usuari (amb rols diferents) accedeixin a un mateix sistema, és imprescindible garantir que només aquells que ho necessitin obtinguin privilegis elevats.
A.9.4.5: Control d'accés al codi font dels programes	Sí	L'Organització requereix que hi hagi un control d'accés al codi font dels programes, especialment degut a que també es duu a terme desenvolupament de software propi.
A.10: Criptografia		
A.10.1: Controls criptogràfics		
A.10.1.1: Política d'usos dels controls criptogràfics	Sí	Existeixen múltiples algoritmes d'encriptació i amb paràmetres de configuració molt variats. És doncs necessari que existeixi una política de seguretat al respecte que indiqui clarament quines regles cal seguir.
A.10.1.2: Gestió de claus	Sí	Les claus d'encriptació han d'ésser gestionades de forma procedimentada. Serà necessari, per exemple, establir un procediment sobre on emmagatzemar-les, sobre quan cal renovar-les, etc.
A.11: Seguretat física i de l'entorn		
A.11.1: Àrees segures		
A.11.1.1: Perímetre de seguretat física	Sí	El fet de disposar de seu física i que la direcció no permet l'accés a persones no involucrades amb l'Organització fa que sigui necessari establir un perímetre, dins el qual només es pot accedir amb acreditació.
A.11.1.2: Controls físics d'entrada	Sí	Són necessaris controls físics per a accedir, d'una banda, a les instal·lacions de l'Organització (es desprèn del control anterior) i, de l'altra, a diverses ubicacions dins de les mateixes, e.g. despatxos o sales de servidors.
A.11.1.3: Seguretat d'oficines, despatxos i recursos	No	No són necessaris més controls de seguretat dins de les oficines i despatxos, més enllà del control d'entrada (e.g. portes tancades amb clau i/o codi), ja contemplats en el control A.11.1.2.
A.11.1.4: Protecció contra les amenaces externes i ambientals	Sí	Amb la finalitat de protegir la seu física i el que s'hi allotja, i per a minimitzar l'impacte en el negoci que situacions negatives externes i ambientals podrien tenir-hi, cal definir procediments per a protegir-se d'aquestes

Control	Aplica	Justificació
		amenaces.
A.11.1.5: El treball en àrees segures	No	No existeixen dins de l'Organització àrees que requereixin d'un nivell de seguretat destacat envers la resta, més enllà del control d'entrada.
A.11.1.6: Àrees de càrrega i descàrrega	No	Els processos de negoci de l'Organització no requereixen càrrega i descàrrega de material de manera sistemàtica. En els casos puntuals que això és necessari, un o més empleats s'encarreguen de rebre el material. I, en tot cas, les àrees restringides estan protegides amb control d'entrada (control A.11.1.2).
A.11.2: Seguretat dels equips		
A.11.2.1: Emplaçament i protecció d'equips	Sí	Els equips han d'estar protegits, tant d'accessos no autoritzats com de possibles amenaces externes o ambientals. Amb aquesta finalitat, la ubicació ha de ser estudiada i escollida de manera apropiada.
A.11.2.2: Instal·lacions de subministrament	Sí	Amb la finalitat de minimitzar l'impacte i/o el temps de resposta en cas d'un incident de seguretat, cal tenir procediments per a afavorir un subministrament ininterromput, e.g. l'ús de SAIs o d'autogeneradors.
A.11.2.3: Seguretat del cablejat	Sí	Tant per a protegir les necessitats del negoci com per a evitar accidents personals, és necessari mantenir un nivell de seguretat adequat amb el cablejat, tant de dades com de subministre elèctric.
A.11.2.4: Manteniment dels equips	Sí	És imprescindible planificar i implementar un manteniment regular de tots els equips de l'Organització, amb múltiples finalitats, com poden ser la disponibilitat o corregir vulnerabilitats.
A.11.2.5: Retirada de materials propietat de la empresa	No	No te especial rellevància el fet que un equip es pugui extreure de les instal·lacions. Les dades més sensibles ho són a un nivell més elevat (a nivell lògic més que no físic), i aquestes potencials fugues d'informació, tot i essent molt rellevants, no augmenten pel fet de trobar-se els equips (e.g. portàtils) dins o fora de les instal·lacions.
A.11.2.6: Seguretat dels equips fora de les instal·lacions	Sí	En els últims anys ha anat incrementant la quantitat d'equips que estan situats fora de les instal·lacions (e.g. al *Cloud*). És necessari,

Control	Aplica	Justificació
		doncs, establir procediments per a mantenir un nivell de seguretat adequat per als mateixos.
A.11.2.7: Reutilització o eliminació segura d'equips	Sí	Tots els equips tenen una vida útil finita, després de la qual aquests són reemplaçats per part de l'Organització. A mode d'evitar la fuga d'informació, és necessari establir procediments d'eliminació segura d'equips.
A.11.2.8: Equip d'usuari desatès	Sí	Un equip en ple funcionament i temporalment desatès és una potencial fuga d'informació. Amb la finalitat de minimitzar aquesta casuística, cal establir controls per a gestionar aquestes situacions (e.g. auto-bloqueig d'equips després de cert temps).
A.11.2.9: Política de lloc de treball ordenat i pantalla neta	No	Es considera que no és imprescindible establir una política sobre com d'ordenat han d'estar els despatxos dels treballadors i contractistes. En quant a evitar fuges d'informació, ja hi ha altres controls que miren d'evitar-ho, com A.9.4.3 per a gestionar les contrasenyes o A.11.2.8 per a bloquejar l'accés als equips.
A.12: Seguretat de les operacions		
A.12.1: Procediments i responsabilitats operacionals		
A.12.1.1: Documentació de procediments d'operació	Sí	És necessari definir de manera formal com s'han de realitzar els diferents procediments del dia a dia, sovint executats per diferents empleats, i amb l'objectiu que aquests es facin de la manera més homogènia possible.
A.12.1.2: Gestió de canvis	Sí	Cal gestionar els canvis d'una manera procedimentada i controlada, incloent en aquesta gestió els aspectes relacionats amb la seguretat de la informació.
A.12.1.3: Gestió de capacitats	Sí	Degut a la naturalesa dels estudis de l'Organització, les capacitats necessàries (e.g. recursos de computació) poden canviar sovint. Cal doncs gestionar els canvis per a donar resposta a aquestes necessitats.
A.12.1.4: Separació dels recursos de desenvolupament, prova i operació	Sí	La separació d'entorns i de recursos és sempre un requisit indispensable quan aquests han d'atendre necessitats diferents. Per exemple, a l'entorn de prova es validaran els sistemes, mentre que al d'operacions no podem permetre'ns discontinuïtats en el servei, alhora

Control	Aplica	Justificació
		que volem tenir-lo protegit contra vulnerabilitats de noves versions (i encara no conegudes).
A.12.2: Protecció contra software maliciós (*malware*)		
A.12.2.1: Controls contra el codi maliciós	Sí	Cal implementar controls per a detectar codi que pugui ser maliciós, ja sigui voluntària o involuntàriament, per a minimitzar el risc de patir un incident de seguretat.
A.12.3: Còpies de seguretat		
A.12.3.1: Còpies de seguretat de la informació	Sí	Disposar de còpies de la informació és indispensable sempre que les dimensions de la seguretat disponibilitat i/o integritat tinguin rellevància per als processos de l'Organització, com és el cas.
A.12.4: Registres i supervisió		
A.12.4.1: Registre d'events	Sí	És necessari l'establiment de procediments de registre d'events, fet que permetrà un seguiment posterior de les activitats en cas necessari.
A.12.4.2: Protecció de la informació del registre	Sí	Aquests registres poden mantenir informació sensible o confidencial, motiu pel qual és necessari que hi hagi controls o altre tipus de protecció per a accedir-hi.
A.12.4.3: Registres d'administració i operació	Sí	És especialment rellevant el registre de les activitats d'administració i operació, ja que mitjançant aquestes es pot alterar substancialment l'estat dels sistemes i, al seu torn, dels processos de negoci.
A.12.4.4: Sincronització del rellotge	Sí	Per a garantir un correcte funcionament dels sistemes, que interactuen entre ells dins de l'Organització i amb altres de fora de la mateixa, cal que hi hagi una sincronització del rellotge que tenen com a referència.
A.12.5: Control del software en explotació		
A.12.5.1: Instal·lació del software en explotació	Sí	Cal controlar i avaluar el software prèviament a passar-lo a una fase productiva, amb especial èmfasi als aspectes relacionats amb la seguretat de la informació.
A.12.6: Gestió de la vulnerabilitat tècnica		
A.12.6.1: Gestió de les vulnerabilitats tècniques	Sí	És necessari gestionar les possibles vulnerabilitats que hi hagi als diversos sistemes, ja sigui detectant-les com mirant de mitigar-les.

Control	Aplica	Justificació
A.12.6.2: Restricció en la instal·lació de software	Sí	Degut al potencial que te el software – tant cap a bé / legítim com cap a malament / il·legítim – és necessari establir controls per a restringir la instal·lació de programari a únicament aquell desitjat.
A.12.7: Consideracions sobre l'auditoria de sistemes d'informació		
A.12.7.1: Controls d'auditoria de sistemes d'informació	Sí	Assolir el nivell de seguretat fixat pels objectius no eximeix a l'Organització de seguir duent a terme controls per avaluar l'evolució del mateix, davant a situacions potencialment canviats. És a dir, cal realitzar auditories (encara que siguin internes) dels sistemes, de forma periòdica i planificada.
A.13: Seguretat de les comunicacions		
A.13.1: Gestió de la seguretat de xarxes		
A.13.1.1: Controls de xarxa	Sí	A l'Organització existeixen diferents actius connectats a la xarxa i que contenen informació, en part confidencial. Per aquest motiu, i perquè hi treballen diferent tipus d'empleats, tant des de les instal·lacions com de forma remota, és necessari establir controls per accedir a la xarxa.
A.13.1.2: Seguretat dels serveis de xarxa	Sí	Amb la finalitat de gestionar les xarxes i els serveis accessibles a través de la mateixa, i fer-ho de manera segura, cal establir mecanismes que ho facilitin.
A.13.1.3: Segregació en xarxes	Sí	Els diferents segments de xarxa de l'Organització tenen finalitats diferents. Degut a això, i a que hem de mirar de exposar els actius el menys possible a potencials amenaces, cal segregar les xarxes.
A.13.2: Intercanvi d'informació		
A.13.2.1: Polítiques i procediments d'intercanvi d'informació	Sí	S'intercanvia informació, tant a nivell intern com amb terceres parts. És necessari doncs que hi hagi procediments que defineixin com s'ha de dur a terme aquest intercanvi, de manera segura.
A.13.2.2: Acords d'intercanvi d'informació	Sí	En el cas d'intercanvis d'informació entre l'Organització i contractistes o altres terceres parts, cal que quedi documentat formalment i de manera vinculant els procediments a seguir (i a no seguir, e.g. publicació d'informació confidencial).

Control	Aplica	Justificació
A.13.2.3: Missatgeria electrònica	Sí	És necessari que s'estableixin uns procediments sobre com s'ha de dur a terme la missatgeria electrònica. En algunes ocasions s'ha de requerir l'ús d'encriptació, tant per motius de confidencialitat, com d'integritat i de no-repudi.
A.13.2.4: Acords de confidencialitat o no revelació	Sí	Relacionat amb el control A.13.2.2, cal que existeixin acords vinculants respecte a la confidencialitat de certes informacions.
A.14: Adquisició, desenvolupament i manteniment dels sistemes d'informació		
A.14.1: Requisits de seguretat en els sistemes d'informació		
A.14.1.1: Anàlisi de requisits i especificacions de seguretat de la informació	Sí	De forma similar al control A.6.1.5, és necessari considerar els requisits de seguretat des de les fases més inicials de creació, adquisició o millora de sistemes.
A.14.1.2: Assegurar els serveis d'aplicacions en xarxes públiques	Sí	Degut a que existeix intercanvi d'informació, de forma automatitzada i sistemàtica, entre l'Organització i altres entitats, és necessari establir controls per assegurar que aquestes dades es transmetin de forma segura.
A.14.1.3: Protecció de les transaccions de serveis d'aplicacions	Sí	Cal garantir que l'intercanvi d'informació entre els diferents serveis existents (pertanyents a la pròpia Organització) també es faci de manera segura. Alguns exemples són les transaccions en bases de dades o l'enviament de dades a serveis FTP.
A.14.2: Seguretat en el desenvolupament i en els processos de suport		
A.14.2.1: Política de desenvolupament segur	Sí	Dins de les activitats de l'Organització, també es desenvolupa software propi. Per aquest motiu, i de forma similar al control A.14.1.1, és necessari establir una política sobre desenvolupament segur.
A.14.2.2: Procediment de control de canvis en sistemes	Sí	Els canvis en els sistemes s'han de realitzar de manera controlada, amb especial èmfasi en els canvis en l'entorn de producció, motiu pel qual cal disposar d'un procediment que ho reguli.
A.14.2.3: Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu	Sí	Com a part final del procés de canvis cal realitzar una avaluació procedimentada sobre quin han estat els resultats i, en cas necessari, prendre mesures per a revertir els canvis.

Control	Aplica	Justificació
A.14.2.4: Restriccions als canvis als paquets de software	Sí	Amb la finalitat de disposar d'un entorn productiu estable, és convenient establir controls sobre quins paquets de software es poden desplegar i quins no (o no sense proves prèvies).
A.14.2.5: Principis d'enginyeria de sistemes segurs	Sí	De forma similar a A.14.1.1 i A.14.2.1, cal establir principis bàsics de seguretat de la informació a l'hora de realitzar les tasques d'enginyeria dels sistemes.
A.14.2.6: Entorn de desenvolupament segur	Sí	Cal disposar d'un entorn segur en el qual realitzar el desenvolupament i on implementar les polítiques definides a A.14.2.1.
A.14.2.7: Externalització del desenvolupament de software	Sí	A l'Organització no només es treballa amb software propi o de tercers, sinó que també es delega el desenvolupament de programari en subcontractistes. És doncs necessari que hi hagi procediments de desenvolupament segur d'aquest software.
A.14.2.8: Proves funcionals de seguretat de sistemes	Sí	A l'hora de realitzar tests, cal avaluar els sistemes també des del punt de vista de la seguretat de la informació.
A.14.2.9: Proves d'acceptació de sistemes	Sí	Les proves esmentades en el control anterior han de finalitzar amb proves d'acceptació (o no) dels sistemes nous o modificats, per a formar part del conjunt global de l'Organització.
A.14.3: Dades de prova		
A.14.3.1: Protecció de les dades de prova	Sí	Sovint és necessari utilitzar dades de prova per a realitzar els tests dissenyats. Aquestes dades, tant si contenen informació sensible com si no, caldrà protegir-les adequadament per a que estiguin disponibles quan es requereixin.
A.15: Relació amb proveïdors		
A.15.1: Seguretat en les relacions amb proveïdors		
A.15.1.1: Política de seguretat de la informació en les relacions amb els proveïdors	Sí	L'Organització fa ús de proveïdors de serveis per a realitzar alguna de les tasques internes (e.g. algunes operacions de xarxes). Per tal d'assegurar que les comunicacions amb els proveïdors es realitzen de forma segura cal establir una política de seguretat al respecte.
A.15.1.2: Requisits de seguretat en contractes amb tercers	Sí	De forma similar al control anterior, també es necessari definir requisits en matèria de seguretat de la informació en referència a les relacions

Control	Aplica	Justificació
		amb terceres parts, com per exemple acords de confidencialitat.
A.15.1.3: Cadena de subministrament de tecnologia de la informació i de les comunicacions	Sí	És necessari establir procediments que controlin la seguretat de la informació durant tota la cadena de subministrament.
A.15.2: Gestió de la provisió de serveis del proveïdor		
A.15.2.1: Control i revisió de la provisió de serveis del proveïdor	Sí	Un cop establerta la política de seguretat (control A.15.1.1), i durant la prestació del servei per part del proveïdor, cal avaluar contínuament que aquest es realitza satisfactòriament i conforme a la política.
A.15.2.2: Gestió de canvis en la provisió del servei del proveïdor	Sí	Cal gestionar els possibles canvis en el proveïdor o en els serveis que aquests proporciona, de manera que es minimitzin els possibles impactes negatius i no se'n vegi afectada la seguretat.
A.16: Gestió d'incidents de seguretat de la informació		
A.16.1: Gestió d'incidents de seguretat de la informació i millores		
A.16.1.1: Responsabilitats i procediments	Sí	Cal definir d'una manera clara i inequívoca quins són els rols, responsabilitats associades i els procediments a seguir en cas d'incidents de seguretat.
A.16.1.2: Notificació dels events de seguretat de la informació	Sí	Com a part dels procediments, és necessari la comunicació d'events de seguretat a les autoritats, parts de l'Organització, proveïdors o terceres parts pertinents.
A.16.1.3: Notificació de punts dèbils de la seguretat	Sí	Cal prendre nota i notificar-se mútuament, per part tant de l'Organització com de proveïdors de servei i tercers, de possibles punts febles o fallades de seguretat que s'identifiquin.
A.16.1.4: Avaluació i decisió sobre els events de seguretat de la informació	Sí	És necessari incloure en els procediments a dur a terme en casos d'events de seguretat mecanismes per avaluar la situació i prendre decisions.
A.16.1.5: Resposta a incidents de seguretat de la informació	Sí	De forma similar al control anterior, cal proporcionar controls per a donar resposta a events que comportin incidents de seguretat de la informació.
A.16.1.6: Aprenentatge dels incidents de seguretat de la informació	Sí	Tot i que mirem de minimitzar l'ocurrència d'incidents de seguretat de la informació, el risc 0 no existeix, i és probable que n'acabin

Control	Aplica	Justificació
		apareixent. En aquest cas és important que, com a mecanisme de millora contínua, mirem d'aprendre d'aquests successos.
A.16.1.7: Recopilació d'evidències	Sí	Cal recopilar i mantenir informació respecte a incidents de seguretat ocorreguts, de manera que es puguin analitzar en un futur i que se n'hi pugui fer referència.
A.17: Aspectes de seguretat de la informació per a la gestió de la continuïtat del negoci		
A.17.1: Continuïtat de la seguretat de la informació		
A.17.1.1: Planificació de la continuïtat de la seguretat de la informació	Sí	És necessari establir un pla de contingència com a mesures d'emergència en el cas que la resta de controls fallin.
A.17.1.2: Implementar la continuïtat de la seguretat de la informació	Sí	Cal que s'implementin les mesures definides en el control anterior, de manera que ajudin a recuperar els processos de negoci de la millor manera possible, en cas que es produeixi un desastre.
A.17.1.3: Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació	Sí	A fi i efecte de detectar possibles deficiències o millores en les mesures de continuïtat de la seguretat de la informació, cal avaluar de forma periòdica els procediments.
A.17.2: Redundàncies		
A.17.2.1: Disponibilitat dels recursos de tractament de la informació	Sí	L'Organització disposa de multitud d'actius, ja siguin en forma d'infraestructura física, servidors, xarxes, software, personal, etc. Una part d'aquests actius són considerats crítics per als processos de negoci. Cal doncs disposar de redundància, per a evitar que una indisponibilitat dels mateixos afecti de manera negativa a l'Organització.
A.18: Compliment		
A.18.1: Compliment dels requisits legals i contractuals		
A.18.1.1: Identificació de la legislació aplicable i dels requisits contractuals	Sí	És imprescindible que s'identifiqui quina legislació aplica a l'Organització i als processos de negoci que es duen a terme, també en quan a les relacions contractuals amb contractistes i tercers.
A.18.1.2: Drets de propietat intel·lectual (DPI)	Sí	Cal definir els drets de propietat intel·lectual del material utilitzat dins de l'Organització, tant per

Control	Aplica	Justificació
		a conèixer formalment com actuar envers informació propietat de tercers, com per a indicar quins són els drets del material creat pels empleats de l'Organització (e.g. software o resultat d'estudis).
A.18.1.3: Protecció dels registres de la organització	Sí	És necessari establir mecanismes de protecció i control d'accés dels registres existents, per a evitar accessos il·legítims.
A.18.1.4: Protecció i privacitat de la informació de caràcter personal	Sí	Alguns processos de l'Organització requereixen el tractament de dades personals. Aquest motiu fa necessari que es defineixin procediments per a protegir aquesta informació i la privacitat de les persones a qui fan referència.
A.18.1.5: Regulació dels controls criptogràfics	Sí	Amb la finalitat d'assegurar el compliment de la legislació a l'hora d'utilitzar control criptogràfics, cal establir procediments que regulin els mateixos.
A.18.2: Revisions de la seguretat de la informació		
A.18.2.1: Revisió independent de la seguretat de la informació	Sí	En quant a realitzar una revisió de la seguretat de la informació, en el sentit més ampli (polítiques, responsabilitats, regulacions, implementacions, controls, avaluacions, etc), sempre resultarà més efectiu i menys influenciat (o amb menys prejudicis) fer-ho de manera independent.
A.18.2.2: Compliment de les polítiques i normes de seguretat	Sí	Cal establir procediments per revisar el compliment de les polítiques i normes de seguretat establertes, de forma periòdica.
A.18.2.3: Comprovació del compliment tècnic	Sí	Cal establir procediments per revisar que les mesures tècniques dissenyades i implementades segueixen assegurant un compliment de les polítiques definides. Igual que en el control anterior, cal fer aquesta revisió de forma periòdica.

Taula 82: Aplicabilitat dels controls ISO/IEC 27002 a l'Organització

19. Annex VIII: Informe d’auditoria de maig de 2022

Control de versions

Versió	Data	Descripció dels canvis
V1	11/05/2022	Versió inicial de l’informe de l’auditoria de maig de 2022

19.1 Introducció

Una de les activitats fonamentals per a dur a terme una avaluació objectiva de l'estat actual de l'SGSI de l'Organització és la realització d'auditories. La realització de les mateixes, programades de forma periòdica i recurrent, proporcionen una visió completa de l'estat de l'SGSI, així com un seguit de conformitats i no-conformitats respecte als objectius a assolir. En el cas de les auditories de l'Organització, l'anàlisi del compliment d'objectius es realitza, d'una banda, sobre els requisits de seguretat definits a l'annex 12. i, d'altra banda, en base al compliment dels diferents dominis de la norma ISO/IEC 27001 [3] i dels controls definits a ISO/IEC 27002 [1]. Finalment, es proporcionen recomanacions de millora que puguin ajudar a reduir el número de no-conformitats.

El present document recull la documentació associada a l'auditoria sobre l'SGSI de l'Organització, realitzada el maig de 2022. En aquest document es troben definits l'abast de l'auditoria – veure 19.2 –, la normativa de referència – veure 19.3 – i l'informe d'auditoria pròpiament – veure 19.4 .

Cal destacar que l'auditoria s'ha realitzat sobre l'estat de l'SGSI un cop han estat aplicades les diferents propostes de projectes descrites a 7. . En conseqüència, els nivells de maduresa analitzats, tant dels dominis de la norma ISO/IEC 27001 com dels controls ISO/IEC 27002, són els definits, respectivament, a 7.7 i 7.8 .

19.2 Abast

L’abast del present informe d’auditoria es centra en documentar de manera exhaustiva els resultats de l’auditoria realitzada sobre l’SGSI de l’Organització durant el maig de 2022. Com a tal, i en concordança amb l’abast determinat al pla director de seguretat, la documentació i els procediments auditats són aquells relacionats amb els següents processos de negoci:

- Processos per a adquisició de dades necessàries per a la realització dels estudis.
- Processos per a tractament i emmagatzematge de les dades i resultats.
- Processos per a la publicació de resultats.

19.3 Normativa de referència

Les diferents auditories de seguretat sobre l'SGSI de l'Organització estan determinades, tant en la forma i programació com en el contingut, pel procediment d'auditories internes definit a l'annex 13. . Aquest procediment defineix quina ha de ser la programació temporal de les auditories (mínim cada 12 mesos), qui n'és el responsable (CISO, *IT Manager* o un responsable d'una altra àrea), quin ha de ser el contingut de les auditories (es defineix el model d'informe d'auditoria), i quins són els passos posteriors a la realització de l'informe (revisió de resultats amb participació de la direcció).

El procediment d'auditories internes, a més, està basat en l'anàlisi de la norma ISO/IEC 27001 [3] i l'aplicació dels controls definits a l'ISO/IEC 27002 [1].

19.4 Informe d’auditoria

El present apartat recull pròpiament l’informe de l’auditoria realitzada sobre l’SGSI de l’Organització, seguint l’estructura del model d’informe d’auditoria definit a l’annex 13. .

19.4.1 Data

L’auditoria de compliment s’ha realitzat durant els dies 9, 10 i 11 de maig de 2022.

19.4.2 Responsable

El responsable de l’auditoria és el CISO de l’Organització.

19.4.3 Nom de l’auditor o auditors

Les diferents activitats d’avaluació de l’SGSI s’han realitzat mitjançant una col·laboració conjunta per part de:

- CISO de l’Organització, amb el suport de treballadors de l’àrea de seguretat.
- *IT Manager* de l’Organització, amb el suport de treballadors de l’àrea d’IT.

19.4.4 Abast

L’abast de l’auditoria de compliment està definit a 19.2 i es centra en els processos de negoci determinats al pla director de seguretat de l’Organització.

19.4.5 Controls auditats

Els controls auditats són tots aquells que apliquen a l’abast de l’SGSI de l’Organització. És a dir, d’entre tots els controls definits a l’ISO/IEC 27002, s’han auditat aquells que resulten rellevants per als processos de negoci de l’Organització, segons l’establert a la declaració d'aplicabilitat – veure annex 18. . La següent taula mostra la valoració de l’equip auditor

sobre cadascun dels controls analitzats (no s'han llistat aquells controls no contemplats a la declaració d'aplicabilitat).

Control	Anàlisi de l'equip auditor
A.5: Polítiques de seguretat de la informació	
A.5.1: Directrius de gestió de la seguretat de la informació	
A.5.1.1: Polítiques per la seguretat de la informació	Existeix una política de seguretat de la informació definida i comunicada a totes les parts interessades. Aquesta política cobreix aspectes d'objectius i estratègia del negoci, marc regulador aplicable, rols i responsabilitats associades, i referencia altres polítiques i reglaments de nivell inferior. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.5.1.2: Revisió de les polítiques per la seguretat de la informació	Existeixen procediments definits de revisió de les polítiques de seguretat de la informació, per part de la direcció i d'altres parts implicades (e.g. CISO). Aquests procediments especifiquen tant la programació temporal com el contingut i metodologia a seguir en les revisions. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.6: Organització de la seguretat de la informació	
A.6.1: Organització interna	
A.6.1.1: Rols i responsabilitats en seguretat de la informació	S'han definit els diferents rols i responsabilitats en l'àmbit de la seguretat de la informació. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.6.1.2: Segregació de tasques	S'han descrit les tasques associades a cadascun dels rols definits, de manera que queda explicitada la segregació de tasques en matèria de seguretat de la informació. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.6.1.3: Contacte amb les autoritats	Existeixen processos informals de contacte amb les autoritats pertinents, e.g. en cas de fuga d'informació. Els procediments, però, es fan de forma individual i sense basar-se en cap documentació existent.

Control	Anàlisi de l'equip auditor
	L'estat d'aquest control no és suficient, i és necessari establir procediments documentats sobre com s'ha d'efectuar el contacte amb les autoritats, en quins casos, i per part de qui.
A.6.1.4: Contacte amb grups d'interès especial	Es duen a terme contactes amb grups d'interès relacionats amb les activitats de l'Organització (e.g. participació en fòrums i xerrades sobre recerca). Tot i així, no existeix una documentació que especifiqui com s'ha de dur a terme aquest contacte. L'estat d'aquest control és millorable. És necessari establir procediments documentats sobre com s'ha de dur a terme el contacte amb grups d'interès per a l'Organització.
A.6.1.5: Seguretat de la informació en la gestió de projectes	Es consideren criteris de seguretat de la informació en la realització i gestió dels diferents projectes que es duen a terme en l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.6.2: Els dispositius mòbils i el teletreball	
A.6.2.1: Política de dispositius mòbils	Existeix una política de dispositius mòbils («Política sobre l'ús de dispositius d'usuari: portàtils, telèfons i *smartphones*»), referenciada a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.6.2.2: Teletreball	S'han definit i establert un conjunt de mesures per a regular i gestionar el teletreball com a possibilitat laboral dins de l'Organització. La documentació corresponent està recollida a la «Política sobre la regulació del teletreball». Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.7: Seguretat relativa als recursos humans	
A.7.1: Abans del treball	
A.7.1.1: Investigació d'antecedents	Com a part del procés de selecció de nous treballadors, es duu a terme una investigació dels possibles antecedents dels mateixos. Degut a la naturalesa de l'Organització, aquest és un procés imprescindible i ineludible. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.

Control	Anàlisi de l'equip auditor
A.7.1.2: Condicions de treball	Les relacions contractuals entre l'Organització i totes aquelles persones o parts interessades (treballadors, contractistes i altres tercers) disposen de clàusules respecte a la seguretat de la informació. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.7.2: Durant el treball	
A.7.2.1: Responsabilitats de gestió	La direcció de l'Organització, delegant si s'escau en els responsables de cadascuna de les diferents àrees de negoci, assegura que s'apliquin les mesures corresponents d'àmbit de seguretat de la informació, segons estan aquestes definides a les polítiques de seguretat de la informació. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.7.2.2: Conscienciació, educació i capacitació en seguretat de la informació	Es duen a terme campanyes de difusió i de conscienciació en matèria de seguretat de la informació, de forma regular i programada, i involucrant totes les parts interessades (treballadors, subcontractistes i terceres parts). D'aquesta manera s'assegura un coneixement actual dels aspectes de seguretat de la informació que afecten a l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.7.2.3: Procés disciplinari	Tot i que hi ha casos de sancions a antics empleats (e.g. per filtració deliberada de dades confidencials), no existeixen procediments documentats sobre com actuar en aquestes situacions. Els responsables de l'Organització actuen, per tant, sense recolzar-se sobre una normativa clara, documentada i comunicada. L'estat d'aquest control no és suficient, i és necessari establir procediments documentats sobre el procés a seguir en cas de mesures disciplinàries, i definir els criteris d'aplicació de les mateixes.
A.7.3: Finalització del treball o canvi de lloc de treball	
A.7.3.1: Responsabilitats davant la finalització o canvi	Està definida l'actualització que pateixen les responsabilitats en casos de canvis de tasques dins de l'Organització (e.g. canvi de rol o canvi de departament), o bé en cas de finalització de contracte laboral (e.g. fi de contracte amb una empresa subcontractada), i la comunicació dels canvis existents a les parts interessades.

Control	Anàlisi de l'equip auditor
	Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.8: Gestió d'actius	
A.8.1: Responsabilitat sobre els actius	
A.8.1.1: Inventari d'actius	L'Organització disposa d'un inventari actualitzat dels diferents actius vinculats als processos de negoci. Un element que constata l'existència d'aquest inventari és l'anàlisi de riscos de seguretat de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.8.1.2: Propietat dels actius	Tots els actius tenen assignats un propietari que, com a tal, s'encarrega de l'inventariat dels mateixos i del seu manteniment. De forma similar al control anterior, l'anàlisi de riscos de seguretat de l'Organització evidencia l'existència de la propietat dels actius. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.8.1.3: Ús acceptable dels actius	Existeix documentació que regula l'ús d'alguns dels tipus d'actiu (veure «Política sobre l'ús de dispositius d'usuari: portàtils, telèfons i *smartphones*»). Tot i així, no es defineix de manera clara, en tots els casos d'ús, i per a tots els tipus d'actius, quin n'és l'ús acceptable segons les normes de l'Organització. L'estat d'aquest control és millorable. És necessari establir polítiques d'ús acceptable per a tots el tipus d'actius existents i en tots els casos d'ús.
A.8.1.4: Devolució d'actius	De forma similar al control anterior, es defineixen els procediments de devolució d'actius per a alguns dels tipus d'actius existents. L'estat d'aquest control és millorable. Cal definir de forma clara i unívoca quina és la política de devolució dels actius, per a tots els tipus existents i en tots els casos d'ús.
A.8.2: Classificació de la informació	
A.8.2.1: Classificació de la informació	S'han definit diferents categories per a classificar la informació que es tracta dins de l'Organització (pública, interna, confidencial). Aquesta classificació i els criteris de cada categoria estan, a més, documentats de forma exhaustiva a la «política sobre la classificació de la informació».

Control	Anàlisi de l'equip auditor
	Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.8.2.2: Etiquetat de la informació	Tot i la definició de les diferents categories d'informació existents, l'etiquetat de la informació no es fa conforme a procediments preestablerts. L'estat d'aquest control és millorable. Cal definir procediments que defineixin com i quan s'ha d'etiquetar la informació, en base a les categories prèviament definides.
A.8.2.3: Manipulació de la informació	Si bé es cert que la informació es gestiona d'una manera o una altra en funció de la categoria a la qual pertany, aquestes diferencies en la gestió (e.g. no enviar per correu electrònic informació confidencial) no es basen en procediments que defineixin la seva manipulació de forma clara i inequívoca. L'estat d'aquest control és millorable. Cal definir procediments que defineixin com s'ha de manipular la informació, en base a la categoria a la qual pertany.
A.8.3: Manipulació dels suports	
A.8.3.1: Gestió de suports extraïbles	La gestió dels suports extraïbles utilitzats durant els processos de negoci de l'Organització es duu a terme d'una forma *best effort* per part dels treballadors. Tot i que aquests són conscients de la importància dels aspectes de la seguretat de la informació, no existeixen procediments que defineixin el detall de com ha de ser aquesta gestió. L'estat d'aquest control és millorable. Cal definir procediments que defineixin, en detall, com s'ha de realitzar la gestió de suports extraïbles.
A.8.3.2: Eliminació de suports	En la majoria de casos dels quals se'n te constància, els suports han estat eliminats de forma conseqüent una vegada ja no són d'utilitat pels processos de negoci de l'Organització (e.g. eliminació d'un llapis de memòria no funcional). Tot i així, no existeixen procediments que especifiquin com i quan s'ha de dur a terme aquesta eliminació. L'estat d'aquest control és millorable. Cal definir procediments que defineixin, en detall, com s'ha de realitzar l'eliminació de suports extraïbles.
A.8.3.3: Suports físics en trànsit	S'ha observat que hi ha situacions, tot i que poc comunes, en les quals s'envien suports físics, ja sigui dins de l'Organització o entre aquesta i una tercera entitat. En aquests casos no hi ha cap normativa generalitzada sobre com cal gestionar els suports. Cada persona realitza la gestió dels mateixos de forma individual

Control	Anàlisi de l'equip auditor
	i seguint el seu propi criteri. L'estat d'aquest control no és suficient, i és necessari establir procediments documentats sobre el procés a seguir en cas de gestió de suports físics en trànsit.
A.9: Control d'accés	
A.9.1: Requisits de negoci pel control d'accés	
A.9.1.1: Política de control d'accés	Existeixen polítiques de control de l'accés a les xarxes i servidors de l'Organització («Reglament general d'accés a la xarxa de l'Organització» i «Política de control d'accés a la informació de l'Organització»), referenciades a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.1.2: Accés a les xarxes i als servidors de xarxa	L'accés a les diferents xarxes i servidors de l'Organització està controlat i limitat exclusivament a aquelles persones i sistemes que, per disseny i política organitzativa, l'han de tenir. Existeixen mesures tècniques que possibiliten la implantació de dit control (e.g. tallafocs, sistemes d'autenticació i autorització o ús de VPNs). Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.2: Gestió d'accés d'usuari	
A.9.2.1: Registre i baixa d'usuari	Existeixen procediments establerts a dur a terme en el cas de baixa d'un usuari (e.g. revocar l'accés del directori actiu als exempleats o subcontractistes que ja no treballin per l'Organització). Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.2.2: Provisió d'accés d'usuari	Existeixen procediments establerts a dur a terme en el cas d'alta d'un nou usuari, o bé en el cas d'extensió de responsabilitats i, per tant, de la necessitat d'accedir a xarxes o servidors de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.2.3: Gestió de privilegis d'accés	Els privilegis d'accés s'assignen o es revoquen, conforme a allò definit a la política de control d'accés, i en funció de les altes i baixes d'usuaris en cada sistema, sempre seguint el principi de

Control	Anàlisi de l'equip auditor
	least privilege. Tot i així, no existeix un procediment especific i documentat per a gestionar els privilegis d'accés. L'estat d'aquest control és millorable. Cal definir un procediment específic per a gestionar els privilegis d'accés.
A.9.2.4: Gestió de la informació secreta d'autenticació dels usuaris	La informació secreta d'autenticació s'emmagatzema i tracta per part dels seus propietaris (dels usuaris) d'una forma conscientment segura. Aquesta gestió, però, es realitza de forma individual per part de cada usuari i sense estar basada en un procediment formal que defineixi els requisits d'aquesta gestió. L'estat d'aquest control és millorable. Cal definir i implementar un procediment de gestió de la informació secreta d'autenticació dels usuaris.
A.9.2.5: Revisió dels drets d'accés d'usuari	Com a part de les revisions periòdiques que es duen a terme en l'Organització, s'avaluen els drets d'accés d'usuari existents i, en cas necessari, s'efectuen les modificacions oportunes. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.2.6: Retirada o reassignació dels drets d'accés	Existeixen procediments per a retirar els drets d'accés a aquelles persones, ja siguin exempleats o subcontractistes, que ja no requereixen de l'accés a un recurs determinat. D'igual forma, també es troben procedimentats els passos a seguir per a realitzar una reassignació de drets d'accés, en cas necessari (e.g. canvi de projecte). Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.3: Responsabilitats de l'usuari	
A.9.3.1: Ús de la informació secreta d'autenticació	La informació secreta d'autenticació – contrasenyes, certificats SSL, identificadors d'usuari – es gestiona de forma segura, tant en el seu emmagatzematge (s'utilitzen gestors de contrasenyes) com en el seu ús (e.g. es fan servir sempre canals encriptats). Existeix, a més, una «política sobre gestió de contrasenyes», referenciada a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.4: Control d'accés a sistemes i aplicacions	
A.9.4.1: Restricció de l'accés a la informació	L'accés a la informació no està suficientment restringit. D'una banda, sí es controla i restringeix l'accés a les xarxes i servidors

Control	Anàlisi de l'equip auditor
	de l'Organització (control A.9.1.2), tant a usuaris com a sistemes i processos. D'altra banda, però, i tot i l'existència de mesures de seguretat en el disseny (*Security by Design*), no sempre es duu a terme una restricció efectiva de tots els accessos a tots els serveis i aplicacions. L'estat d'aquest control és millorable. Cal avaluar de forma sistemàtica tots els possibles accessos a la informació, a través de tots els tipus d'actius i fent ús de tots els canals – físic, visual, telefònic, electrònic, etc –. Un cop identificades les vies d'accés, cal aplicar el definit a la «Política de control d'accés a la informació de l'Organització».
A.9.4.2: Procediments d'inici de sessió	Hi ha establerts procediments d'inici de sessió segurs com a part del sistema de control d'accés als recursos de l'Organització, exemples dels quals són: usuari/contrasenya, ús de certificats SSL i ús de tickets *Kerberos*. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.4.3: Sistema de gestió de contrasenyes	Les contrasenyes es gestionen mitjançant un gestor de contrasenyes especialitzat, el qual està programat amb criteris segurs (e.g. longitud mínima, ha de contenir caràcters especials). Les contrasenyes, a més, s'han d'actualitzar com a mínim un cop al trimestre – veure «Política sobre gestió de contrasenyes». En cas contrari, l'usuari que en fa ús queda deshabilitat fins a nova actualització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.4.4: Ús d'utilitats amb privilegis del sistema	Les utilitzats s'executen per defecte sense privilegis de sistema (o privilegis d'administrador). Puntualment, és possible executar utilitats amb privilegis de sistema. Per a fer-ho, cal demanar permís explícit al departament d'IT i, prèvia anàlisi de l'*IT Manager*, el permís s'atorga a un usuari i un dispositiu en concret, i durant un temps finit. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.9.4.5: Control d'accés al codi font dels programes	Actualment és possible accedir al codi font de gairebé qualsevol desenvolupament realitzat com a part dels processos de negoci de l'Organització. Sovint, a més, és possible fer-ho amb permisos d'escriptura, possibilitant no només la violació de la dimensió de confidencialitat, sinó també la de l'integritat de la informació.

Control	Anàlisi de l'equip auditor
	L'estat d'aquest control no és suficient, i és necessari implementar un control d'accés al codi font dels programes, especialment sobre aquell codi desenvolupat com a part dels processos de negoci de l'Organització.
A.10: Criptografia	
A.10.1: Controls criptogràfics	
A.10.1.1: Política d'usos dels controls criptogràfics	S'ha definit una política d'ús dels controls criptogràfics – veure «Política sobre el controls criptogràfics», referenciada a la política de seguretat de la informació de l'Organització. En aquesta política es defineixen els algoritmes d'encriptació permesos, juntament amb un conjunt de paràmetres de configuració (e.g. longitud mínima de clau). Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.10.1.2: Gestió de claus	Existeixen procediments que defineixen com s'han de gestionar les claus criptogràfiques durant tot el seu cicle de vida, incloent els criteris a seguir per a la seva generació i actualització periòdiques. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.11: Seguretat física i de l'entorn	
A.11.1: Àrees segures	
A.11.1.1: Perímetre de seguretat física	Les instal·lacions de l'Organització es troben delimitades dins d'un perímetre de seguretat, de forma que queda clarament diferenciat què pertany a les instal·lacions i què no. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.11.1.2: Controls físics d'entrada	Existeixen controls físics a l'hora d'accedir a les instal·lacions de l'Organització i, dins de les mateixes, per accedir a alguns edificis i/o sales determinades. D'aquesta forma és possible assegurar l'accés a únicament personal autoritzat. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.11.1.4: Protecció contra les amenaces externes i ambientals	S'han implantat mesures de protecció contra amenaces externes i ambientals (e.g. separació de sales amb materials anti-incendi). A més, existeix una consciència especialment elevada envers a amenaces externes, probablement influenciada per l'antiguitat de l'Organització i els diferents esdeveniments a que ha hagut de fer front.

Control	Anàlisi de l’equip auditor
	Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.11.2: Seguretat dels equips	
A.11.2.1: Emplaçament i protecció d’equips	La disposició dels diferents equips dins de les instal·lacions de l’Organització respon a un disseny avaluat i documentat. S’han implantat, a més, mecanismes de protecció dels equips, segons queda definit al «reglament de mecanismes de protecció d’oficines i equipament físic». Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.11.2.2: Instal·lacions de subministrament	Existeixen partides pressupostàries destinades de forma concreta a garantir els subministraments necessaris per a dur a terme els processos de negoci de l’Organització: electricitat, telecomunicacions, aigua i gas. Aquests recursos, juntament amb la planificació existent, garanteixen el servei ininterromput (o amb temps d’interrupció molt baixos) dels subministres. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.11.2.3: Seguretat del cablejat	Tot el cablejat comprovat, *in situ*, està disposat de forma segura, amb atenció especial sobre possibles afectacions a treballadors o a la integritat física d'altre equipament (e.g. cablejat de subministrament elèctric). Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.11.2.4: Manteniment dels equips	El manteniment dels diferents equips de l’Organització, tant el software com el hardware, es duu a terme de forma regular i programada, en base a l’establert a la «política sobre actualitzacions de sistemes», la qual es troba referenciada a la política de seguretat de la informació de l’Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.11.2.6: Seguretat dels equips fora de les instal·lacions	Existeixen polítiques documentades sobre les mesures a seguir per a mantenir un nivell de seguretat adequat sobre els equips de fora de les instal·lacions de l’Organització. Exemples d’aquestes polítiques són la «política sobre l’ús de serveis en el *Cloud*» i la «política sobre la regulació del teletreball», ambdues referenciades a la política de seguretat de la informació de l’Organització.

Control	Anàlisi de l'equip auditor
	Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.11.2.7: Reutilització o eliminació segura d'equips	A l'hora d'eliminar equips (o parts d'ells, e.g. el disc dur), es duen a terme mesures per a esborrar de forma segura la informació existent, de forma que es mantingui la confidencialitat de la mateixa. Alguns exemples són: eliminació total dels discs o *wipe* i destrucció completa de cintes d'emmagatzematge. Aquestes mesures, però, es prenen per iniciativa individual i no estan basades en procediments documentats. L'estat d'aquest control és millorable. Cal establir procediments documentats de reutilització o eliminació segura d'equips.
A.11.2.8: Equip d'usuari desatès	Els usuaris són conscients del risc que representa per a la seguretat de l'Organització un equip desatès i que no es protegeixi correctament. Es duen a terme mesures com e.g. bloquejar els equips, o inclús apagar-los, quan aquests es troben desatesos. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.12: Seguretat de les operacions	
A.12.1: Procediments i responsabilitats operacionals	
A.12.1.1: Documentació de procediments d'operació	Existeixen procediments d'operació dels diferents processos de negoci de l'Organització. Les tasques definides en els procediments estan en concordança amb allò definit pel control ISO/IEC 27002 (instal·lació i configuració de sistemes, còpies de seguretat, etc). Tot i així, aquestes procediments no són homogenis per a projectes de caire similar de l'Organització, sinó que cada projecte te definits els seus propis procediments. L'estat d'aquest control és millorable. Cal establir normes generals de redacció de procediments d'operacions, de manera que els diferents projectes facin ús de metodologies i tècniques similars a l'hora de definir les seves operacions.
A.12.1.2: Gestió de canvis	No existeixen procediments documentats i estandaritzats de gestió de canvis. Les activitats per a tractar amb els canvis existents en els sistemes de l'Organització es duen a terme de manera acordada entre les parts interessades, però sense basar-se en documentació que reguli com ha de ser-ne la gestió. L'estat d'aquest control no és suficient, i és necessari establir procediments de gestió de canvis, a poder ser d'una forma

Control	Anàlisi de l'equip auditor
	homogeneïtzada per a processos similars dins de l'Organització.
A.12.1.3: Gestió de capacitats	Es duen a terme planificacions de capacitats en els recursos necessaris per a suportar els processos de negoci de l'Organització. A més, també existeixen procediments per a avaluar i adaptar els recursos en funció de les necessitats canviants d'aquests processos. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.12.1.4: Separació dels recursos de desenvolupament, prova i operació	Existeix una separació física (e.g. amb tallafocs) i lògica (e.g. amb configuracions de subxarxes) dels diferents recursos, en funció del tipus d'activitat que s'hi desenvolupi. Així, l'Organització disposa dels entorns diferenciats de: desenvolupament, prova o validació i operació. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.12.2: Protecció contra software maliciós (*malware*)	
A.12.2.1: Controls contra el codi maliciós	Existeixen controls per a detectar i prevenir codi maliciós. Tot i així, aquests controls no estan presents de forma generalitzada a tots els servidors de l'Organització, sinó que depèn de la proactivitat dels gestors de cada projecte el fet que aquests s'implementin o no. L'estat d'aquest control és millorable. Cal implementar els controls contra el codi maliciós de manera generalitzada a tots els processos de l'Organització.
A.12.3: Còpies de seguretat	
A.12.3.1: Còpies de seguretat de la informació	Es realitzen còpies de seguretat de la informació de forma regular i programada, i segons l'establert a la «política de còpies de seguretat», la qual es troba referenciada a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.12.4: Registres i supervisió	
A.12.4.1: Registre d'events	S'efectua el registre d'alguns tipus d'events, sobretot els generats pels serveis i aplicacions dels processos de l'Organització (e.g. logs i altres alertes). Manca un registre sistemàtic de les activitats realitzades pels diferents usuaris dels sistemes.

Control	Anàlisi de l'equip auditor
	L'estat d'aquest control és millorable. Cal crear procediments que regulin el registre de tot tipus d'activitats, tant d'usuaris com de serveis i aplicacions, i implementar-ho allà on encara no s'estigui duen a terme.
A.12.4.2: Protecció de la informació del registre	La informació dels diferents registres existents pot ésser accedida sovint sense cap control d'accés (més enllà del control d'accés dels servidors on s'han generat els registres). Aquesta situació posa en perill les propietats de confidencialitat, integritat i disponibilitat de la informació. L'estat d'aquest control no és suficient, i és necessari protegir la informació del registre enfront d'accessos i manipulacions no autoritzats.
A.12.4.3: Registres d'administració i operació	De forma similar al control A.12.4.1, s'efectua el registre d'alguns tipus d'accions, però no es registren de manera sistemàtica totes les activitats relacionades amb l'administració i operació dels sistemes de l'Organització. L'estat d'aquest control és millorable. Cal crear procediments que regulin el registre de totes les accions d'administració i operació rellevants, i implementar-ho allà on encara no s'estigui duen a terme.
A.12.4.4: Sincronització del rellotge	Tots els sistemes de l'Organització estan sincronitzats temporalment mitjançant l'ús de servidors NTP. Per a facilitar la comunicació i evitar incerteses o dubtes a l'hora de correlar moments temporals, es fa servir sempre l'hora en format UTC. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.12.5: Control del software en explotació	
A.12.5.1: Instal·lació del software en explotació	Existeixen procediments documentats sobre els requisits del software per a passar a entorns de producció o explotació. Aquest, a més, s'avalua exhaustivament abans de ser operacionalitzat, tant des d'una vessant funcional com considerant aspectes de seguretat de la informació. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.12.6: Gestió de la vulnerabilitat tècnica	
A.12.6.1: Gestió de les vulnerabilitats tècniques	Es duen a terme algunes mesures per a gestionar les vulnerabilitats tècniques dels sistemes utilitzats en l'Organització (e.g. escaneig de vulnerabilitats, subscripció a llistes de seguretat i actualitzacions en cas necessari). Tot i així, no existeixen

Control	Anàlisi de l'equip auditor
	procediments exhaustius i documentats que defineixin tot el procés de gestió de les mateixes. L'estat d'aquest control és millorable. Cal crear procediments que defineixin el procés de gestió de vulnerabilitats tècniques i implementar-ne les mesures resultants.
A.12.6.2: Restricció en la instal·lació de software	Existeix documentació procedimental sobre quin tipus de software està permès utilitzar dins de l'àmbit de l'Organització i quin no ho està. Es pot trobar informació al respecte a la «política sobre ús de software a l'Organització», referenciada a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.12.7: Consideracions sobre l'auditoria de sistemes d'informació	
A.12.7.1: Controls d'auditoria de sistemes d'informació	Es duen a terme auditories periòdiques i programades sobre el SGSI de l'Organització. Es planifiquen totes les activitats a realitzar, amb especial èmfasi i cura en aquelles accions que tinguin associat un risc d'impacte en els processos de negoci. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.13: Seguretat de les comunicacions	
A.13.1: Gestió de la seguretat de xarxes	
A.13.1.1: Controls de xarxa	Existeixen mesures tècniques per a controlar l'accés a les diferents xarxes de l'administració (e.g. tallafocs i encaminadors), en les quals resideixen els servidors que allotgen informació rellevant pels processos de negoci de l'Organització. La documentació rellevant es troba definida en polítiques, e.g. al «reglament general d'accés a la xarxa de l'Organització», referenciada a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.13.1.2: Seguretat dels serveis de xarxa	S'identifiquen i descriuen els diferents mecanismes de seguretat destinats a protegir els serveis que s'allotgen a les diferents xarxes de l'Organització. La documentació corresponent es troba definida en polítiques com el «reglament general d'accés a la xarxa de l'Organització» i el «reglament de desplegament de serveis d'informació a una xarxa accessible (DMZ)», ambdós referenciats a la política de seguretat de la informació de l'Organització.

Control	Anàlisi de l'equip auditor
	Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.13.1.3: Segregació en xarxes	Existeix una segregació de les xarxes clara i definida, en funció de criteris de funcionalitat, seguretat i el/s projecte/s al qual donen servei. Un exemple d'aquesta segregació és l'ús de xarxes desmilitaritzades o DMZ per a l'accés públic als serveis de publicació de resultats. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.13.2: Intercanvi d'informació	
A.13.2.1: Polítiques i procediments d'intercanvi d'informació	S'han definit i documentat polítiques i procediments d'intercanvi d'informació, tal i com es pot observar a la «política sobre comunicacions dins de l'Organització i amb entitats externes», referenciada a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.13.2.2: Acords d'intercanvi d'informació	Existeixen acords d'intercanvi d'informació entre l'Organització i terceres parts, en el cas que es transmeti informació considerada confidencial. Els ISA són exemples d'aquest tipus d'acords. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.13.2.3: Missatgeria electrònica	Es regula l'ús de la missatgeria electrònica, tant dins de l'Organització com per a comunicacions amb terceres entitats, de manera que aquesta es realitzi de forma segura. La normativa corresponent es troba recollida al «reglament d'ús del correu electrònic», referenciat a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.13.2.4: Acords de confidencialitat o no revelació	Existeixen acords de confidencialitat o no revelació (d'informació interna o confidencial) entre l'Organització i terceres entitats. Sovint aquestes clàusules es troben recollides en els propis acords d'intercanvi d'informació. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.14: Adquisició, desenvolupament i	

Control	Anàlisi de l'equip auditor
manteniment dels sistemes d'informació	
A.14.1: Requisits de seguretat en els sistemes d'informació	
A.14.1.1: Anàlisi de requisits i especificacions de seguretat de la informació	El disseny i desenvolupament de nous processos i productes contemplen aspectes relacionats amb la seguretat de la informació. Es tenen en compte conceptes de *Security by Design* a l'hora d'encarar anàlisis de requisits. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.14.1.2: Assegurar els serveis d'aplicacions en xarxes públiques	Els serveis de l'Organització que contemplen l'enviament d'informació a través de xarxes públiques han estat dissenyats de manera que aquest trànsit s'efectuï de forma segura. Hi ha implementats mecanismes d'encriptació i autenticació (e.g. VPN) per a tal efecte. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.14.1.3: Protecció de les transaccions de serveis d'aplicacions	De forma similar al control anterior, l'intercanvi d'informació en les transaccions dels diferents serveis d'aplicacions de l'Organització també estan protegides amb mesures tècniques, a fi i efecte de garantir les propietats de seguretat de confidencialitat, integritat i disponibilitat. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.14.2: Seguretat en el desenvolupament i en els processos de suport	
A.14.2.1: Política de desenvolupament segur	S'han definit i documentat procediments per a dur a terme un desenvolupament segur dels nous sistemes. La documentació corresponent es pot trobar a la «política de desenvolupament segur», referenciada a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.14.2.2: Procediment de control de canvis en sistemes	Es duen a terme procediments de control en el cas de canvis en els sistemes. Aquests procediments, però, no estan basats en una regulació generalitzada per als canvis de l'Organització, sinó que varien en funció del projecte i de les persones implicades en el mateix. L'estat d'aquest control és millorable. Cal crear procediments

Control	Anàlisi de l'equip auditor
	que regulin, de manera generalitzada, quines són les activitats a considerar en cas de canvis en els sistemes de l'Organització.
A.14.2.3: Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu	De forma similar al control anterior, i com a part final del procés de canvis, es duen a terme revisions tècniques de les aplicacions per a validar si les modificacions del sistema operatiu són satisfactòries o si, pel contrari, s'han de revertir. Aquestes revisions varien en funció del projecte i de les persones implicades en el mateix. L'estat d'aquest control és millorable. Cal crear procediments que regulin, de manera generalitzada, les revisions tècniques de les aplicacions després de canvis del sistema operatiu en què es sustenten.
A.14.2.4: Restriccions als canvis als paquets de software	Es duen a terme restriccions en el cas d'actualització dels paquets de software existents, tant per a corregir o millorar funcionalitats existents com per afegir-ne de noves. Aquestes restriccions no es duen a terme en tots els casos (e.g. sí en sistemes RedHat però no en sistemes CentOS), ni estan basades en procediments que regulin de forma clara i unívoca com s'han de restringir els canvis. L'estat d'aquest control és millorable. Cal crear procediments que defineixin quins restriccions cal aplicar en cada canvi de paquet de software.
A.14.2.5: Principis d'enginyeria de sistemes segurs	S'apliquen principis d'enginyeria de sistemes segurs a l'hora de tractar amb els serveis i aplicacions, com a part dels conceptes de *Security by Design* aplicats a l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.14.2.6: Entorn de desenvolupament segur	Es disposa d'un entorn de desenvolupament segur, tant pel que respecte a la dimensió de confidencialitat (e.g. cal superar un control per obtenir accés) com pel que respecte a les dimensions d'integritat i disponibilitat d'altres entorns. Això és així, ja que el desenvolupament s'efectua en un entorn completament aïllat dels entorns de prova o validació i d'operacions. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.14.2.7: Externalització del desenvolupament de software	El desenvolupament d'una part del software necessari per als processos de negoci de l'Organització està subcontractat a terceres empreses. En aquests casos, els aspectes de seguretat de la informació no sempre s'avaluen amb la mateixa importància que els aspectes funcionals del software.

Control	Anàlisi de l'equip auditor
	L'estat d'aquest control és millorable. Cal crear procediments que defineixin quins requisits de seguretat cal exigir a les empreses subcontractistes, alhora que especifiquin els criteris d'acceptació del software.
A.14.2.8: Proves funcionals de seguretat de sistemes	Per als nous sistemes i de forma prèvia la operacionalització dels mateixos, es duen a terme tant proves funcionals com proves de seguretat. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.14.2.9: Proves d'acceptació de sistemes	Com a part constitutiva de les proves del control anterior, també es realitzen proves d'acceptació dels sistemes, el resultat de les quals determinarà si aquests poden ésser operacionalitzats o si, pel contrari, requereixen del compliment de criteris de seguretat. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.14.3: Dades de prova	
A.14.3.1: Protecció de les dades de prova	Existeixen mesures de protecció de les dades de prova generades (e.g. el control d'accés als servidors on s'allotgen algunes d'aquestes dades). Tot i així, no existeixen procediments ni mecanismes que protegeixin les dades d'una forma generalitzada i per a tots els projectes de l'Organització. L'estat d'aquest control és millorable. Cal crear procediments i implementar mesures que protegeixin totes les dades de prova, de forma generalitzada i independentment del projecte que les genera.
A.15: Relació amb proveïdors	
A.15.1: Seguretat en les relacions amb proveïdors	
A.15.1.1: Política de seguretat de la informació en les relacions amb els proveïdors	S'ha creat i documentat una política que defineix com han de ser les relacions amb els proveïdors, també en matèria de seguretat de la informació: «política sobre la contractació i tracte amb proveïdors», referenciada a la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.15.1.2: Requisits de seguretat en contractes amb tercers	De forma similar al control A.14.2.7, es consideren alguns aspectes de seguretat en el tracte amb proveïdors. Tot i així, sovint no se li dona el mateix valor als requisits de seguretat que

Control	Anàlisi de l'equip auditor
	a aquells de caràcter funcional. L'estat d'aquest control és millorable. Cal definir els requisits de seguretat a considerar en el tracte amb proveïdors i dotar-los de la mateixa importància que els requisits de caràcter funcional.
A.15.1.3: Cadena de subministrament de tecnologia de la informació i de les comunicacions	No existeixen procediments documentats que incloguin els requisits de seguretat rellevants per a la cadena de subministrament amb proveïdors. L'estat d'aquest control no és suficient, i és necessari establir procediments que defineixin els requisits de seguretat per a la cadena de subministrament amb proveïdors.
A.15.2: Gestió de la provisió de serveis del proveïdor	
A.15.2.1: Control i revisió de la provisió de serveis del proveïdor	S'efectuen revisions periòdiques i programades de la provisió dels serveis del proveïdor. S'avalua el nivell de servei proporcionat, així com les incidències i anomalies de l'últim període. Existeixen, a més, SLAs que defineixen quins són els llindars acceptables en cada cas. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.15.2.2: Gestió de canvis en la provisió del servei del proveïdor	De forma similar al control A.14.2.2, es duen a terme certes activitats per a gestionar el canvis, en aquest cas en la provisió de serveis. Aquestes activitats, però, no estan basades en un procediment generalitzat per als canvis en la provisió del servei del proveïdor, sinó que varien en funció del proveïdor, del projecte i de les persones implicades en el mateix. L'estat d'aquest control és millorable. Cal crear procediments que regulin, de manera generalitzada, quines són les activitats a considerar en cas de canvis en la provisió del servei del proveïdor.
A.16: Gestió d'incidents de seguretat de la informació	
A.16.1: Gestió d'incidents de seguretat de la informació i millores	
A.16.1.1: Responsabilitats i procediments	S'han definit els diferents rols i responsabilitats en l'àmbit de la seguretat de la informació – veure el document de «gestió de rols i responsabilitats», així com procediments per a gestionar els possibles incidents de seguretat. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.

Control	Anàlisi de l'equip auditor
A.16.1.2: Notificació dels events de seguretat de la informació	Com a part dels procediments en cas d'events de seguretat de la informació, es documenten les accions de notificació dels mateixos. Existeixen, a més, campanyes de conscienciació periòdiques on es recorda la metodologia a seguir. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.16.1.3: Notificació de punts dèbils de la seguretat	Els procediments establerts contemplen la notificació dels punts dèbils de seguretat detectats. Existeixen, a més, campanyes de conscienciació periòdiques on es recorda la metodologia a seguir. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.16.1.4: Avaluació i decisió sobre els events de seguretat de la informació	Els procediments documentats contemplen l'avaluació dels events de seguretat de la informació i, en funció de criteris predefinits, ajuden a l'hora de prendre una decisió sobre si es tracta d'incidents de seguretat. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.16.1.5: Resposta a incidents de seguretat de la informació	Existeixen procediments de gestió d'incidents de seguretat de la informació, tal i com s'esmenta als controls anteriors d'aquesta mateixa àrea. Tot i així, aquests procediments no són exhaustius (no es contempla tota la casuística possible a l'hora de donar una resposta als incidents) ni estan basats en metodologies reconegudes internacionalment (com podria ser ITIL). L'estat d'aquest control és millorable. Cal estendre els procediments, de manera que considerin totes les casuístiques possibles. A mode opcional, es poden adaptar els procediments a les bones pràctiques definides al marc de treball ITIL [26].
A.16.1.6: Aprenentatge dels incidents de seguretat de la informació	Els incidents de seguretat s'avaluen de forma periòdica en les diverses revisions existents dins de l'Organització, concretament en les revisions per direcció i en aquelles que es realitzen dins l'àmbit del comitè de seguretat de la informació. A més, el pla director de seguretat de l'Organització també preveu la realització d'auditories internes i externes. De l'anàlisi dels incidents ocorreguts en el passat en les diferents revisions, i de les mesures preses com a conseqüència dels mateixos, podem constatar que el present control es troba en un nivell de maduresa de 5 (OPTIMITZAT).
A.16.1.7: Recopilació d'evidències	Es recopilen algunes evidències dels incidents de seguretat

Control	Anàlisi de l'equip auditor
	ocorreguts. Tanmateix, aquesta recopilació no es realitza en tots els casos, ni en base a procediments establerts, sinó que s'acostuma a fer amb caràcter individual. L'estat d'aquest control no és suficient, i és necessari establir procediments que defineixin com i quan s'han de recopilar les evidències sobre incidents de seguretat de la informació.
A.17: Aspectes de seguretat de la informació per a la gestió de la continuïtat del negoci	
A.17.1: Continuïtat de la seguretat de la informació	
A.17.1.1: Planificació de la continuïtat de la seguretat de la informació	Existeixen algunes mesures destinades a mantenir la continuïtat del negoci i, concretament, a garantir la continuïtat de la seguretat de la informació a l'Organització. Tot i així, no s'ha documentat un pla de contingència complet, de manera que es determinin les necessitats de seguretat de la informació de l'Organització i les mesures a prendre per a reduir el temps de recuperació dels sistemes. L'estat d'aquest control és millorable. Cal elaborar el pla de contingència de l'Organització.
A.17.1.2: Implementar la continuïtat de la seguretat de la informació	S'implementen diferents mesures tècniques i organitzatives que afavoreixen la continuïtat de la seguretat de la informació de l'Organització, en cas de desastre. Com es deprèn del control A.17.1.1, però, manca documentació formal i exhaustiva respecte als mecanismes implementats. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.17.1.3: Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació	Les mesures tècniques i organitzatives implementades, així com la documentació existent (tot i que no hi ha un pla complet de contingència) es verifiquen i revisen de forma periòdica. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.17.2: Redundàncies	
A.17.2.1: Disponibilitat dels recursos de tractament de la informació	Es garanteix la disponibilitat dels recursos necessaris per al tractament de la informació en l'àmbit de la realització dels processos de negoci de l'Organització, en tant en quan s'ha dissenyat i implementat una redundància dels diferents equips i serveis, especialment d'aquells considerats crítics. Una avaluació i revisió contínua ajudarà a evolucionar a un

Control	Anàlisi de l'equip auditor
	nivell 5 (OPTIMITZAT) de maduresa.
A.18: Compliment	
A.18.1: Compliment dels requisits legals i contractuals	
A.18.1.1: Identificació de la legislació aplicable i dels requisits contractuals	S'ha identificat la legislació aplicable als processos de negoci de l'Organització, així com els requisits contractuals amb les diferents parts interessades. Es pot trobar informació documentada al respecte al marc regulador de la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.18.1.2: Drets de propietat intel·lectual (DPI)	S'han identificat els drets de propietat intel·lectual d'aplicació als processos de negoci de l'Organització. Per les característiques dels processos, aquests drets es centren principalment en el software desenvolupat i en els resultats dels estudis realitzats. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.18.1.3: Protecció dels registres de la organització	Existeixen algunes mesures de protecció dels registres de l'Organització. Tanmateix, aquestes es duen a terme de manera individual i sense basar-se en procediments generals establerts a tal efecte. L'estat d'aquest control no és suficient, i és necessari establir procediments que defineixin els nivells de protecció dels registres de l'Organització, i implementar-ne els mecanismes tècnics que ho possibilitin.
A.18.1.4: Protecció i privacitat de la informació de caràcter personal	Es defineixen els nivells de protecció i privacitat de la informació de caràcter personal, principalment regulats a través del reglament general de protecció de dades personals o GDPR. Es pot trobar informació documentada al respecte al marc regulador de la política de seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.18.1.5: Regulació dels controls criptogràfics	Existeixen procediments documentats que defineixen les característiques dels controls criptogràfics a utilitzar, i ho fan acorde a la legislació vigent. Es pot trobar informació documentada a la «política sobre el controls criptogràfics», referenciada a la política de seguretat de la informació de l'Organització.

Control	Anàlisi de l'equip auditor
	Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.18.2: Revisions de la seguretat de la informació	
A.18.2.1: Revisió independent de la seguretat de la informació	Es duen a terme revisions independents de la seguretat de la informació de l'Organització, tant en forma de revisions periòdiques (per part de personal no involucrat directament, e.g. per part de la direcció) com en forma d'auditories, tant internes com externes. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.18.2.2: Compliment de les polítiques i normes de seguretat	Les diferents revisions definides i programades de l'SGSI de l'Organització, juntament amb els indicadors existents, possibiliten l'avaluació del compliment de les polítiques i normes de seguretat. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
A.18.2.3: Comprovació del compliment tècnic	De forma similar al control anterior, les diferents revisions de l'SGSI de l'Organització possibiliten l'avaluació del compliment tècnic de les mesures definides i implementades. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.

Taula 83: Auditoria sobre els controls ISO/IEC 27002 a l'Organització

19.4.6 Conformitat de l'SGSI amb els requisits de seguretat de l'Organització

En el present apartat de l'auditoria de seguretat de l'Organització l'equip auditor analitza el compliment dels requisits de seguretat establerts, definits com a objectius de seguretat dins de la política de seguretat de la informació.

Objectiu:
Garantir un nivell de protecció adequat de la informació i dels actius i serveis que la sustenten

Anàlisi de l'equip auditor:
Les mesures tècniques i organitzatives existents en l'àmbit de la seguretat de la informació possibiliten una

protecció conforme als nivells planificats per part de l'Organització. Els indicadors existents (e.g. número d'incidents) serveixen com a dades objectives per a demostrar que el nivell de protecció és l'adequat.

Objectiu:
Garantir la continuïtat dels processos de negoci de l'Organització

Anàlisi de l'equip auditor:
Els processos de negoci de l'Organització han seguit produint els resultats esperats (publicació dels resultats provinents dels estudis realitzats) durant tot l'històric analitzat, tot i / gràcies a l'SGSI de l'Organització. Per tant, es pot afirmar que es garanteix la continuïtat dels processos de negoci de l'Organització.

Objectiu:
Garantir la confidencialitat, integritat i disponibilitat de la informació de l'Organització i de totes les parts implicades en els processos de negoci

Anàlisi de l'equip auditor:
El fet que s'hagi garantit la continuïtat dels processos de negoci de l'Organització, juntament amb el baix número d'incidències en matèria de seguretat de la informació, permet afirmar que s'han garantit les dimensions clàssiques de la seguretat en les parts implicades de l'Organització: la confidencialitat, la integritat i la disponibilitat de la informació.

Objectiu:
Assegurar el compliment del marc legal aplicable i dels contractes establerts

Anàlisi de l'equip auditor:
Les revisions – i, en cas necessari, adaptacions – de les definicions del marc legal i dels contractes establerts, així com l'absència d'incidències relacionades amb aspectes legals i contractuals en els registres històrics de l'Organització, permeten afirmar que hi ha un compliment dels mateixos.

Objectiu:
Assegurar la conformitat amb l'estàndard internacional ISO/IEC 27001

Anàlisi de l'equip auditor:
La realització i positiva valoració de la present auditoria de seguretat permet assegurar la conformitat amb la norma ISO/IEC 27001, així com amb els controls definits a l'annex de la mateixa (controls ISO/IEC 27002).

Objectiu:
Garantir l'aplicació de processos de millora contínua en el marc de la seguretat de la informació

Anàlisi de l'equip auditor:
L'Organització ha dissenyat i implementat processos de millora contínua en el marc de la seguretat de la informació, en forma de revisions periòdiques i auditories, tal i com demostren els diferents registres existents i les mesures tècniques i organitzatives de millora que se'n desprenen de les mateixes.

Objectiu:
Garantir el coneixement i aplicació de la política de seguretat de la informació per part de totes les parts interessades i de tots els empleats de l'Organització

Anàlisi de l'equip auditor:
Existeixen campanyes de difusió i conscienciació que, entre d'altres, possibiliten el coneixement de la política de seguretat de la informació existent per part de tots els treballadors, subcontractistes i altres parts implicades en els processos de negoci de l'Organització. La realització de dites campanyes, juntament amb l'alt nivell de conscienciació que mostren tots els empleats, permet afirmar que es garanteix el coneixement

i aplicació de la política.

Objectiu:
Garantir la revisió periòdica de la política de seguretat de la informació per part del Comitè de seguretat

Anàlisi de l'equip auditor:
Existeixen procediments de revisió per part de diferents rols i grups d'empleats dins de l'Organització, incloent el Comitè de seguretat. Aquests procediments, juntament amb els registres i anotacions de les diferents reunions ocorregudes, permeten constatar que hi ha una revisió periòdica de la política de seguretat de la informació de l'Organització.

Taula 84: Auditoria sobre els objectius de seguretat de l'Organització

19.4.7 Conformitat de l'SGSI amb la norma ISO/IEC 27001

Mitjançant l'auditoria de seguretat s'avaluen els graus d'adequació dels diferents requisits de la norma ISO/IEC 27001, els quals es mostren en la següent taula.

Requisits	Anàlisi de l'equip auditor
4: L'Organització i el Context	
4.1: Entenent l'organització i el seu context	
4.1.1: Estan identificats els objectius del SGS Sistema de Gestió de la Seguretat de la Informació?	Els objectius de l'SGSI de l'Organització estan identificats i documentats a la política de seguretat de la informació. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
4.1.2: S'han identificat les qüestions internes i externes relacionades amb la seguretat de la informació?	Els aspectes que tenen un impacte en la seguretat de la informació, tant aquells que són intrínsecs a l'Organització (interns) com aquelles que provenen de terceres parts (externs), s'han identificat durant l'elaboració del pla director de seguretat de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
4.1.3: S'han identificat com les parts internes i externes poden suposar amenaces o riscos per a la seguretat de la informació?	Les parts internes i externes han estat identificades, tal i com s'esmenta en el punt anterior. Tanmateix, hi ha una manca d'indicadors respecte a les amenaces o riscos que aquestes poden suposar per a la seguretat de la informació de l'SGSI de l'Organització. L'estat d'aquest requisit és millorable. Es poden definir indicadors sobre l'afectació de les parts internes i externes, de manera que es possibiliti un nivell de maduresa 4

Requisits	Anàlisi de l’equip auditor
	(GESTIONAT I MESURABLE) i, posteriorment, un nivell de maduresa 5 (OPTIMITZAT).
4.2: Expectatives de les parts interessades	
4.2.1: S'han identificat les parts interessades?	De forma similar al requisit 4.1.3, s’han identificat les parts interessades però no existeixen indicadors que possibilitin un nivell de maduresa 4 (GESTIONAT I MESURABLE).
4.2.2: Hi ha un llistat de requisits sobre Seguretat de la Informació de les parts interessades?	Els requisits de seguretat de la informació de les parts interessades estan identificats i documentats a la política de seguretat de la informació i en les diferents polítiques referenciades en la primera. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
4.2.3: Hi ha un llistat de requisits sobre Seguretat de la Informació referent a reglaments, requisits legals i requisits contractuals?	Els requisits sobre reglaments, requisits legals i requisits contractuals es troben definits a la política de seguretat de la informació de l’Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
4.3: Abast del SGSI	
4.3.1: S'ha determinat l'abast del SGS i se'n conserva informació documentada?	L’abast de l’SGSI de l’Organització està definit en el pla director de seguretat, així com en les diverses polítiques i reglaments. L’estat d’aquest requisit és millorable. Es poden definir indicadors que possibilitin un nivell de maduresa 4 (GESTIONAT I MESURABLE) i, posteriorment, un nivell de maduresa 5 (OPTIMITZAT).
4.4: Sistema de Gestió de la Seguretat de la informació	
4.4.1: El sistema de Gestió de Seguretat de la informació SGSI està establert, implementat i es revisa de manera planificada considerant oportunitats de millora?	Efectivament, l’SGSI de l'Organització està definit (en el pla director de seguretat), implementat i es revisa de forma programada i continua. A més, en les revisions es consideren oportunitats de millora de l’SGSI. Després de vàries iteracions, es considera que l’estat del present requisit és de maduresa total, o nivell 5 (OPTIMITZAT).
5: Lideratge	
5.1: Lideratge i compromís	
5.1.1: S'han establert objectius de la Seguretat de la Informació d'acord amb els objectius del negoci?	Els objectius de seguretat de la informació estan establerts en concordança amb els objectius de negoci de l’Organització, i es troben definits a la política de seguretat de la informació.

Requisits	Anàlisi de l'equip auditor
	Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
5.1.2: La direcció proveeix dels recursos materials i humans necessaris per al compliment dels objectius del SGSI?	La direcció s'implica en molts dels procediments, campanyes i activitats relacionades amb la seguretat de la informació. Degut a aquesta participació i a la conscienciació pròpia sobre la importància de l'SGSI per a l'Organització, la direcció assigna els recursos necessaris per a l'assoliment dels objectius marcats. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
5.1.3: La direcció revisa directament l'eficàcia de l'SGSI per garantir que es compleixen els objectius de l'SGSI?	La direcció revisa de forma directa, tant de forma exclusiva com en participació conjunta amb altres empleats (e.g. amb el CISO i l'*IT Manager*), l'eficàcia de l'SGSI. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
5.2: Política de la Seguretat de la Informació	
5.2.1: S'ha definit una política de seguretat de la informació?	S'ha elaborat i documentat una política de seguretat de la informació. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
5.2.2: S'ha establert un marc que permeti establir objectius?	No existeix un marc definit i documentat com a pas previ a la definició dels objectius de seguretat de l'SGSI de l'Organització. Existeixen, però, els objectius de negoci de l'Organització, els quals ajuden a l'establiment dels objectius de seguretat. L'estat d'aquest requisit és millorable. Cal establir un marc que defineixi les bases per a establir els objectius de seguretat de l'SGSI de l'Organització.
5.2.3: S'ha comunicat la política de seguretat de la informació a les parts interessades i a tota l'empresa?	La política de seguretat de la informació s'ha comunicat, en l'àmbit de campanyes de difusió i conscienciació, a totes les parts interessades de l'Organització, tant a treballadors interns com a subcontractistes i terceres parts. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
5.2.4: Es manté informació documentada de la política de l'SGSI i dels seus objectius?	Es manté un control de versions de la política de seguretat de la informació de l'Organització definida. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.

Requisits	Anàlisi de l'equip auditor
5.3: Rols i Responsabilitats	
5.3.1: S'han assignat les responsabilitats i les autoritats sobre la Seguretat de la Informació?	Les responsabilitats i autoritats en matèria de seguretat de la informació s'han definit en l'àmbit del pla director de seguretat de l'Organització, e.g. al document de gestió de rols i responsabilitats. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
5.3.2: S'han comunicat convenientment les responsabilitats i les autoritats per a la Seguretat de la Informació?	Les responsabilitats i autoritats en matèria de seguretat de la informació s'han comunicat, en l'àmbit de campanyes de difusió i conscienciació, a totes les parts interessades de l'Organització, tant a treballadors interns com a subcontractistes i terceres parts. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
6: Planificació	
6.1: Tractament de Riscos i Oportunitats	
6.1.1: El pla per abordar riscos i oportunitats considera les expectatives de les parts interessades en relació amb la seguretat de la informació?	Existeix un anàlisi de riscos de l'Organització, però no hi ha un pla concret per abordar i tractar (o gestionar) els riscos existents. En conseqüència, i tot i que existeixen idees i propostes de millora de la seguretat de la informació, no es pot afirmar que es consideren les expectatives de les parts interessades de forma completa i exhaustiva. L'estat d'aquest requisit és millorable. Cal establir un pla per abordar els riscos detectats.
6.1.2: S'identifiquen i analitzen els riscos mitjançant un mètode d'avaluació i d'acceptació de riscos?	Es duen a terme anàlisis de riscos mitjançant mètodes d'avaluació i acceptació reconeguts – en concret, es fa ús de la metodologia Magerit. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
6.1.3: S'ha definit un procés de tractament de riscos?	No s'ha definit un procés de tractament de riscos. Sí que existeixen, però, i com s'indica al requisit 6.1.1, idees i propostes de millora de la seguretat de la informació, associades als anàlisis de riscos que es fan en l'àmbit dels processos de negoci de l'Organització. L'estat d'aquest requisit és millorable. Cal establir un procés de tractament dels riscos detectats.
6.1.4: S'han establert criteris per elaborar una declaració d'aplicabilitat?	S'ha elaborat una declaració d'aplicabilitat dels controls ISO/IEC 27002 sobre els processos de negoci de l'Organització.

Requisits	Anàlisi de l’equip auditor
	Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
6.1.5: Es manté informació documentada dels punts anteriors?	Els punts anteriors estan definits en un conjunt de documents, pertanyents al pla de seguretat de l’Organització i amb controls de versions. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
6.2: Planificació per aconseguir objectius	
6.2.1: S'han establert objectius de la Seguretat de la Informació mesurables i d'acord amb els objectius del negoci?	Els objectius de seguretat de la informació són mesurables, avaluables, i estan definits en base als objectius del negoci de l’Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
6.2.2: Els objectius de la Seguretat de la Informació estan planificats mitjançant? - Assignació de responsabilitats - Cronograma d'execució temporal - Mètode d'avaluació	S’han establert les següents propietats dels objectius de seguretat de la informació: - Assignació de responsabilitats - Mètode d'avaluació En canvi, no s’ha definit una planificació temporal sobre l’execució de les tasques per assolir els objectius fixats. Aquest requisit de la norma te, per tant, potencial de millora.
6.2.3: S'han integrat els objectius de la Seguretat de la Informació als processos de l'organització tenint en compte les funcions principals dins de l’Organització?	Els objectius de seguretat de la informació han estat definits tenint en consideració els diferents rols i responsabilitats establerts en l’Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
7: Suport	
7.1: Recursos	
7.1.1: S'identifiquen i assignen els recursos necessaris per a l'SGSI?	Una de les conseqüències positives de l’involucrament en les reunions de l’àmbit de la seguretat de la informació, per part de la direcció de l’Organització, és l’assignació dels recursos necessaris per a la implementació i gestió de l’SGSI. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
7.2: Competència	
7.2.1: S'avalua la competència en matèries de seguretat de la informació per a	Prèviament a la contractació de personal (o reassignació d’empleats en altres projectes), es duu a terme una avaluació de

Requisits	Anàlisi de l'equip auditor
persones que efectuen tasques que puguin afectar la seguretat?	les competències dels mateixos en matèries de seguretat de la informació, de manera que s'assegura la idoneïtat (o no) dels empleats per a la realització de dites tasques. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
7.2.2: Es manté informació actualitzada sobre la competència del personal?	Es disposa d'informació documentada sobre la competència del personal, e.g. en els currículums dels empleats. Aquesta informació, però, no sempre es manté actualitzada. Tampoc existeixen procediments que defineixin com s'ha de dur a terme l'emmagatzematge i actualització de la informació rellevant. L'estat d'aquest requisit de la norma no és suficient, i és necessari establir procediments que defineixin quina informació personal s'ha d'emmagatzemar, en quin format, quines consideracions de seguretat i privacitat s'han de seguir, i quina és la freqüència d'actualització necessària.
7.3: Conscienciació	
7.3.1: El personal està involucrat i és conscient del seu paper a la Seguretat de la Informació?	El personal, tant els empleats de l'Organització com els subcontractistes i altres tercers, estan conscienciats de la importància de la seguretat de la informació a l'hora d'assolir els objectius de negoci dels processos de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
7.3.2: Hi ha consciència dels danys que es poden produir de no seguir les pautes de la Seguretat de la Informació?	De forma similar al requisit anterior, tot el personal està també conscienciat de l'impacte negatiu que l'omissió dels reglaments sobre seguretat de la informació podria tenir sobre els processos de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
7.4: Comunicació	
7.4.1: Es comunica la política de la Seguretat de la Informació amb les responsabilitats de cadascú?	La política de seguretat de la informació es dona a conèixer a tot aquell personal, tant intern de l'Organització com subcontractistes i altres tercers, en l'àmbit de campanyes de difusió i conscienciació. Aquesta comunicació inclou les responsabilitats en matèria de seguretat associades a cada rol. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
7.4.2: Hi ha un procés per comunicar les deficiències o males pràctiques en la seguretat de la informació?	Existeixen processos documentats per comunicar les deficiències o males pràctiques en la seguretat de la informació.

Requisits	Anàlisi de l'equip auditor
	Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
7.5: Informació Documentada	
7.5.1: Es disposa de la documentació requerida per la norma més la requerida per l'organització incloent-hi? - La política de la seguretat de la informació i l'abast del sistema de gestió - Els processos principals de la seguretat de la informació - Els documents exigits per la Norma ISO 27001 incloent registres - Els documents propis de seguretat de la informació identificats per l'empresa (instruccions tècniques etc.)	La documentació requerida existeix i s'ha posat a disposició del present grup d'auditors. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
7.5.2: Hi ha un control documental on es verifica? - Qui publica el document - Qui ho autoritza i com es revisen - Formats i Suports de publicació - El seu emmagatzematge i protecció	Existeix un cert control documental, en tant en quan hi ha un control de versions i s'estableix el responsable de custodiar cada document. D'altra banda, però, no sempre s'especifica qui és l'encarregat de revisar el document ni d'autoritzar-lo. Tampoc es verifica en tots els casos quins són els mecanismes de protecció (e.g. control d'accés) dels documents. L'estat d'aquest requisit és millorable. Cal establir un procediment per definir de forma sistemàtica totes les característiques del control de documents.
7.5.3: Es controlen els documents d'origen extern?	Es duu a terme un cert control dels documents d'origen extern, e.g. documentant-ne la font. Aquest control – limitat – es realitza de forma diferent a cadascun dels projectes de l'Organització. L'estat d'aquest requisit és millorable. Cal establir un procediment per determinar de forma generalitzada quins controls cal realitzar als documents d'origen extern.
8: Operació	
8.1: Control Operacional	
8.1.1: Els processos de seguretat de la informació estan documentats per controlar que es realitzen segons el planificat?	Existeix documentació dels processos que tenen a veure amb la seguretat de la informació. Aquesta documentació, però, no sempre és homogènia per a projectes de caire similar de l'Organització, fet que dificulta poder realitzar un control i comparació d'objectius. L'estat d'aquest control és millorable. Cal establir documentació homogeneïtzada per als processos de seguretat de la informació, que en faciliti el seu control.

Requisits	Anàlisi de l'equip auditor
8.1.2: Hi ha un procés per avaluar els riscos a la Seguretat de la Informació abans de realitzar canvis en el Sistema de Gestió o processos de Seguretat?	Existeixen processos per avaluar els riscos a la seguretat de la informació de l'Organització que poden suposar canvis en sistemes existents, ja siguin en software o en hardware. En base al resultat d'aquesta avaluació es pren la decisió d'efectuar el canvi (o no). Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
8.1.3: S'estableixen mesures i plans per mitigar els riscos a la Seguretat de la Informació davant de canvis realitzats?	Es duen a terme mesures per a mitigar els riscos detectats en canvis dels sistemes. Aquestes mesures, però, no es basen en una planificació generalitzada, sinó que es realitzen de forma individual i en base a coneixement propi, ja sigui d'un o més empleats. L'estat d'aquest control és millorable. Cal establir procediments generalitzats de mitigació de riscos.
8.1.4: S'identifiquen i es controlen els processos externalitzats quant als riscos per a la Seguretat de la Informació?	Existeixen mecanismes de control dels processos externalitzats, tant en quan a la funcionalitat dels mateixos com en quan als riscos que aquests representen per a la seguretat de la informació de l'Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
8.2: Anàlisi de riscos de la Seguretat de la Informació	
8.2.1: S'ha establert un procés documentat d'anàlisi i d'avaluació de riscos per a la seguretat de la informació on s'identifiqui? - El propietari del risc - La importància del risc o nivell d'impacte - La probabilitat d'ocurrència	Existeix un procés documentat sobre quina és la metodologia a seguir a l'hora de realitzar anàlisis de riscos de l'SGSI de l'Organització. A més, existeix documentació respecte a anàlisis ja realitzats, on s'identifica: - El propietari del risc - La importància del risc o nivell d'impacte - La probabilitat d'ocurrència Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
8.3: Tractament de riscos de la Seguretat de la Informació	
8.3.1: S'ha implementat un pla de tractament de risc on? - Els propietaris del risc estan informats i han aprovat el pla - Es documenten els resultats	Es duen a terme revisions dels riscos detectats i categoritzats en l'anàlisi de riscos. En aquestes revisions, entre d'altres, s'avaluen els riscos presentats. No existeix, en canvi, un pla de tractament de risc documentat sobre quin és el procediment generalitzat a seguir a l'hora de gestionar els riscos. L'estat d'aquest control és millorable. Cal definir i implementar

Requisits	Anàlisi de l’equip auditor
	un pla de tractament del risc.
8.3.2: S'identifiquen tots els controls necessaris per mitigar el risc justificant-ne l'aplicació?	S’han identificat els controls a utilitzar per mitigar els riscos detectats en l’anàlisi de riscos. Tanmateix, no existeixen indicadors que permetin avaluar de manera objectiva l’eficàcia d’aquests controls en la reducció real del risc. Aquesta és, per tant, una oportunitat de millora del present requisit, possibilitant un nivell de maduresa 4 (GESTIONAT I MESURABLE) i, posteriorment, un nivell de maduresa 5 (OPTIMITZAT).
8.3.3: Es documenta el nivell d'aplicació de tots els controls que cal aplicar?	Com s’indica a les observacions del requisit anterior, s’han identificat els controls que cal aplicar. En quant al nivell d’aplicació dels controls, però, aquest no sempre queda explicitat juntament amb la rellevància (o no) del control. Aquesta manca de definició del requisit, entesa també com a falta d’indicadors, impossibilita que el requisit es trobi en un nivell de maduresa 4 (GESTIONAT I MESURABLE)
9: Avaluació de l'exercici	
9.1: Seguiment i mesurament	
9.1.1: S'ha establert un procés continu de monitorització dels aspectes clau de la seguretat de la informació tenint en compte els controls per a la seguretat de la informació?	Existeixen processos documentats per a monitoritzar diversos aspectes de l’SGSI de l’Organització, fent ús dels indicadors existents i de forma continua (o seguint els períodes establerts). Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
9.1.2: S'ha establert un procés documentat per avaluar els resultats dels mesuraments i que aquests resultats són presos en compte pels responsables tant dels processos com de la Seguretat de la informació?	Existeixen procediments de revisions periòdiques, involucrant a persones responsables de l’Organització amb capacitat de presa de decisions. En aquestes revisions s’avaluen els resultats dels mesuraments i es prenen les decisions que es consideren més favorables per a l’SGSI de l’Organització, en base a l’històric existent i als procediments definits. Es te constància de vàries iteracions d’aquestes revisions, motiu pel qual es considera un nivell 5 (OPTIMITZAT) del present requisit de la norma.
9.2: Auditories Internes	
9.2.1: S'ha establert una programació d'auditories internes i assignat responsables?	S’han dissenyat i programat auditories internes de forma periòdica, amb assignació de responsabilitats de preparació i realització de la mateixa, i revisió de resultats. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
9.2.2: L'abast i els requisits s'han definit per a l'informe d'auditoria?	S’han definit l’abast i els requisits dels informes d’auditoria. Una avaluació i revisió contínua ajudarà a evolucionar a un

Requisits	Anàlisi de l'equip auditor
	nivell 5 (OPTIMITZAT) de maduresa.
9.2.3: Es consideren accions correctives i propostes de canvi als informes d'auditoria?	El model d'informe d'auditoria contempla accions correctives (o no-conformitats) i propostes de millora. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
9.3: Informe de Revisió per la Direcció	
9.3.1: Hi ha una programació per als informes de la direcció i hi ha constància de la seva realització periòdica?	S'han dissenyat i programat revisions per la direcció, de forma periòdica. Existeix constància de revisions realitzades amb anterioritat i, de fet, l'anàlisi de temes revisats anteriorment és un dels punts a tractar en l'agenda de les reunions. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
9.3.2: Es documenten els resultats dels informes i la direcció s'implica tant en el coneixement com en la presa de decisions sobre els aspectes crucials per al SGSI?	Existeixen procediments per a documentar els resultats de les reunions de revisions per la direcció. A l'hora de prendre decisions, la direcció de l'Organització n'és un actor indispensable, tal i com ho defineix el «procediment de revisió per direcció». Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
10: Millora	
10.1: No Conformitats i accions correctives	
10.1.1: Hi ha un procediment documentat per identificar i registrar les no-conformitats i el seu tractament?	Les no-conformitats de l'SGSI de l'Organització s'identifiquen mitjançant la realització de revisions periòdiques – com la present auditoria –, en les que es dedica una secció de les mateixes a llistar les discrepàncies amb el que estableixen els requisits de la norma ISO/IEC 27001 i els controls ISO/IEC 27002. A més, es suggereix quines són les activitats necessàries per tractar les mancances detectades. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.
10.1.2: Dins de les accions correctives hi ha una diferenciació entre accions correctives sobre la no-conformitat i sobre les causes de la mateixa?	En l'estat actual de les revisions de l'SGSI de l'Organització, les accions correctives es centren en identificar les no-conformitats i mirar de proposar solucions per a tractar les mancances detectades. No es duu a terme, en canvi, un anàlisi de les causes subjacents de les no-conformitats. L'estat d'aquest requisit de la norma no és suficient, i és necessari establir procediments per a realitzar un anàlisi de les

Requisits	Anàlisi de l’equip auditor
	causes subjacents de les no-conformitats.
10.2: Millora continua	
10.2.1: Hi ha un procés per garantir la millora contínua de l'SGSI identificant les oportunitats de millora?	Existeixen processos que garanteixen un monitoratge i avaluació continua de l’SGSI de l’Organització. Amb aquests elements, i degut a que es planifiquen i s’implementen les millores detectades en les reunions d’avaluació de l’estat de l’SGSI, es pot afirmar que hi ha un procés establert de millora contínua dins de l’Organització. Una avaluació i revisió contínua ajudarà a evolucionar a un nivell 5 (OPTIMITZAT) de maduresa.

Taula 85: Auditoria sobre els requisits de la norma ISO/IEC 27001 a l’Organització

19.4.8 No-conformitats detectades

Dels anteriors apartats de l’informe d’auditoria es desprenen les següents no-conformitats, classificades en funció de la criticitat de l’incompliment, de forma descendent: no-conformitat major, no-conformitat menor i observacions.

No-conformitats majors:

No s’ha identificat cap no-conformitat major.

No-conformitats menors:

A continuació es llisten les no-conformitats menors detectades, juntament al control o requisit de la norma a la que fan referència, i a l’acció correctiva necessària en cada cas.

- Control A.6.1.3: Cal establir procediments documentats sobre com s’ha d'efectuar el contacte amb les autoritats pertinents, en quins casos, i per part de qui.

- Control A.6.1.4: És necessari establir procediments documentats sobre com s’ha de dur a terme el contacte amb grups d’interès per a l’Organització.

- Control A.7.2.3: És necessari establir procediments documentats sobre el procés a seguir en cas de mesures disciplinàries, i definir els criteris d’aplicació de les mateixes.

- Control A.8.1.3: És necessari establir polítiques d'ús acceptable per a tots el tipus d'actius existents i en tots els casos d'ús.

- Control A.8.1.4: Cal definir de forma clara i unívoca quina és la política de devolució dels actius, per a tots els tipus existents i en tots els casos d'ús.

- Control A.8.2.2: Cal definir procediments que defineixin com i quan s'ha d'etiquetar la informació, en base a les categories prèviament definides.

- Control A.8.2.3: Cal definir procediments que defineixin com s'ha de manipular la informació, en base a la categoria a la qual pertany.

- Control A.8.3.1: Cal definir procediments que defineixin, en detall, com s'ha de realitzar la gestió de suports extraïbles.

- Control A.8.3.2: Cal definir procediments que defineixin, en detall, com s'ha de realitzar l'eliminació de suports extraïbles.

- Control A.8.3.3: És necessari establir procediments documentats sobre el procés a seguir en cas de gestió de suports físics en trànsit.

- Control A.9.2.3: Cal definir un procediment específic per a gestionar els privilegis d'accés.

- Control A.9.2.4: Cal definir i implementar un procediment de gestió de la informació secreta d'autenticació dels usuaris.

- Control A.9.4.1: Cal aplicar la restricció a l'accés de la informació a través de tots els canals.

- Control A.9.4.5: És necessari implementar un control d'accés al codi font dels programes, especialment sobre aquell codi desenvolupat com a part dels processos de negoci de l'Organització.

- Control A.11.2.7: Cal establir procediments documentats de reutilització o eliminació segura d'equips.

- Control A.12.1.1: Cal possibilitar un mesurament i una gestió adequada dels procediments d'operació.

- Control A.12.1.2: És necessari establir procediments de gestió de canvis.

- Control A.12.2.1: Cal implementar els controls contra el codi maliciós de manera generalitzada a tots els processos de l'Organització.

- Control A.12.4.1: Cal crear procediments que regulin el registre de tot tipus d'activitats, tant d'usuaris com de serveis i aplicacions, i implementar-ho allà on encara no s'estigui duen a terme.

- Control A.12.4.2: És necessari protegir la informació del registre enfront d'accessos i manipulacions no autoritzats.

- Control A.12.4.3: Cal crear procediments que regulin el registre de totes les accions d'administració i operació rellevants, i implementar-ho allà on encara no s'estigui duen a terme.

- Control A.12.6.1: Cal crear procediments que defineixin el procés de gestió de vulnerabilitats tècniques i implementar-ne les mesures resultants.

- Control A.14.2.2: Cal crear procediments que regulin, de manera generalitzada, quines són les activitats a considerar en cas de canvis en els sistemes de l'Organització.

- Control A.14.2.3: Cal crear procediments que regulin, de manera generalitzada, les revisions tècniques de les aplicacions després de canvis del sistema operatiu en què es sustenten.

- Control A.14.2.4: Cal crear procediments que defineixin quins restriccions cal aplicar en cada canvi de paquets de software.

- Control A.14.2.7: Cal crear procediments que defineixin quins requisits de seguretat cal exigir a les empreses subcontractistes, alhora que especifiquin els criteris d'acceptació del software.

- Control A.14.3.1: Cal crear procediments i implementar mesures que protegeixin totes les dades de prova, de forma generalitzada i independentment del projecte que les genera.

- Control A.15.1.2: Cal definir els requisits de seguretat a considerar en el tracte amb proveïdors i dotar-los de la mateixa importància que els requisits de caràcter funcional.

- Control A.15.1.3: És necessari establir procediments que defineixin els requisits de seguretat per a la cadena de subministrament amb proveïdors.

- Control A.15.2.2: Cal crear procediments que regulin, de manera generalitzada, quines són les activitats a considerar en cas de canvis en la provisió del servei del proveïdor.

- Control A.16.1.5: Cal estendre els procediments, de manera que considerin totes les casuístiques possibles.

- Control A.16.1.7: És necessari establir procediments que defineixin com i quan s'han de recopilar les evidències sobre incidents de seguretat de la informació.

- Control A.17.1.1: Cal elaborar el pla de contingència de l'Organització.

- Control A.18.1.3: És necessari establir procediments que defineixin els nivells de protecció dels registres de l'Organització, i implementar-ne els mecanismes tècnics que ho possibilitin.

- Requisit de la norma 5.2.2: Cal establir un marc que defineixi les bases per a establir els objectius de seguretat de l'SGSI de l'Organització.

- Requisit de la norma 6.1.1: Cal establir un pla per abordar els riscos detectats.

- Requisit de la norma 6.1.3: Cal establir un procés de tractament dels riscos detectats.

- Requisit de la norma 6.2.2: Cal definir una planificació temporal sobre l'execució de les tasques per assolir els objectius fixats.

- Requisit de la norma 7.2.2: És necessari establir procediments que defineixin quina informació personal s'ha d'emmagatzemar, en quin format, quines consideracions de seguretat i privacitat s'han de seguir, i quina és la freqüència d'actualització necessària.

- Requisit de la norma 7.5.2: Cal establir un procediment per definir de forma sistemàtica totes les característiques del control de documents.

- Requisit de la norma 7.5.3: Cal establir un procediment per determinar de forma generalitzada quins controls cal realitzar als documents d'origen extern.

- Requisit de la norma 8.1.1: Cal establir documentació homogeneïtzada per als processos de seguretat de la informació, que en faciliti el seu control.

- Requisit de la norma 8.1.3: Cal establir procediments generalitzats de mitigació de riscos.

- Requisit de la norma 8.3.1: Cal definir i implementar un pla de tractament del risc.

- Requisit de la norma 10.1.2: És necessari establir procediments per a realitzar un anàlisi de les causes subjacents de les no-conformitats.

Observacions:

A continuació es llisten les observacions de l'equip auditor:

- Molts controls i requisits de la norma es troben ja a un nivell 4 de maduresa (GESTIONAT I MESURABLE) i disposen de les condicions per a evolucionar més endavant a un nivell 5 (OPTIMITZAT). Per a fer-ho, cal dur a terme una avaluació i revisió continua dels mateixos.

- Requisits de la norma 4.1.3, 4.2.1, 4.3.1, 8.3.2 i 8.3.3: Es poden definir indicadors clars i objectius, de manera que es possibiliti un nivell de maduresa 4 (GESTIONAT I MESURABLE) i, posteriorment, un nivell de maduresa 5 (OPTIMITZAT).

19.4.9 Recomanacions de millora

Com a part dels resultats de la realització de la present auditoria de seguretat, i a més de les accions correctives necessàries per al tractament de les no-conformitats detectades – veure 19.4.8 –, l'equip auditor presenta les següents recomanacions de millora de l'SGSI de l'Organització:

- Es recomana continuar amb les avaluacions i revisions regulars dels controls de seguretat ISO/IEC 27002 i de l'estat dels requisits de la norma ISO/IEC 27001, tal i com ja es realitza en la majora de casos.

- En quant al control Control A.9.4.1, es recomana avaluar de forma sistemàtica tots els possibles accessos a la informació, a través de tots els tipus d'actius i fent ús de tots els canals – físic, visual, telefònic, electrònic, etc –. Un cop identificades les vies d'accés, cal aplicar allò definit a la «Política de control d'accés a la informació de l'Organització».

- Amb la finalitat de millorar els controls A.12.1.1, A.12.1.2, A.14.2.2, A.14.2.3 i A.15.2.2, es recomana aplicar una estandarització dels procediments per als diferents projectes i proveïdors existents dins de l'abast dels processos de l'Organització.

- Com a possibilitat de millora respecte a la gestió d'incidents de seguretat de la informació, es recomana la lectura i aplicació de les bones pràctiques proporcionades al marc de treball ITIL [26].