Implantació d'un SGSI basat en la ISO 27001 en una ONG del Tercer Sector

Nom Estudiant: Marc Vilalta Parra

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

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

Data Lliurament: 9 de gener de 2023

FITXA DEL TREBALL FINAL

Títol del treball:	*Implantació d'un SGSI*
Nom de l'autor:	*Marc Vilalta Parra*
Nom del consultor/a:	*Igor Ruiz Agúndez*
Nom del PRA:	*Carles Garrigues Olivella*
Data de lliurament (mm/aaaa):	*01/2023*
Titulació o programa:	Màster Universitari en Ciberseguretat i Privadesa (MUCIP)
Àrea del Treball Final:	*Sistemes de Gestió de la Seguretat de la Informació*
Idioma del treball:	*Català*
Paraules clau	*SGSI, ISO 27001, Anàlisi*

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

L'estudi de com fer la implementació d'un SGSI en una ONG del tercer sector és l'objectiu d'aquest treball, l'organització representada és fictícia, tot i que esta sustentada sobre una ONG real.

Assegurar la informació, es vital en l'àmbit social, i la ISO 27001 ens proporciona aquests mecanismes, per tant el treball es basa en la implementació del SGSI en tot l'àmbit empresarial en que s'ofereixen serveis essencials als usuaris i que tenen relació directe amb els sistemes d'informació. L'estudi de com fer aquest implementació en una ONG del tercer sector és l'objectiu d'aquest treball, l'organització representada és fictícia, tot i que esta sustentada sobre una ONG real.

Per realitzar el treball em seguit la Norma ISO 27001 i una metodologia d'anàlisi de risc basada en Magerit. Cal destacar l'elaboració d'una política de Seguretat que fins el moment era inexistent a l'Organització.

Els resultats obtinguts són esperançadors i tot i que l'objectiu inicial era una mica ambiciós quasi s'aconsegueix, caldrà seguir treballant i aprofundir en alguns aspectes.

La conclusió és que cal molta experiència i un bon assessorament en el procés de implementació d'un SGSI i la ISO, però que val molt la pena l'esforç. Apostar i donar suport a la incorporació d'aquest mètode és una decisió encertada per part de la direcció.

Abstract (in English, 250 words or less):

The study of how to implement an SGSI in a third sector NGO is the objective of this work, the organization represented is fictitious, although it's based on a real NGO.
Securing information is vital in the social sphere, and ISO 27001 provides us with these mechanisms, therefore the work is based on the implementation of the SGSI throughout the business sphere in which essential services are offered to users and which have direct relationship with information systems. The study of how to implement this in a third sector NGO is the objective of this work, the organization represented is fictitious, although it is based on a real NGO.
To carry out the work I followed the ISO 27001 Standard and a risk analysis methodology based on Magerit. It is worth noting the elaboration of a Security policy which, until now, was non-existent in the Organization.

The results obtained are hopeful and although the initial objective was a bit ambitious it has almost been achieved, it will be necessary to continue working and deepen some aspects.

The conclusion is that a lot of experience and good advice is needed in the process of implementing an ISMS and ISO, but that it is well worth the effort. Betting on and supporting the incorporation of this method is a wise decision on the part of the management.

Índex

Llista de figures

Llista de taules

1. Introducció

1.1 Context i justificació del Treball

Les tecnologies de la informació cada cop són més importants en la societat i evolucionen molt ràpidament, en les empreses aquestes tecnologies també són cada cop més presents. Per tant, la informació és un bé molt preuat que s'ha de cuidar i protegir.

En els sector social, en el que es mou l'ONG és de vital importància la protecció de la informació, ja que en la majoria de casos aquesta informació és de caràcter personal i en molts casos sensible, havent de donar compliment al GPDR (*General Data Protection Regulation*), Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016 i la LOPD/GDD (*Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales*), Llei Orgànica 3/2018, de 5 de desembre de 2018.

1.2 Objectius del Treball

Tal i com s'ha dit la informació, les dades, és l'actiu més valuós de l'organització, la dependència que es té dels serveis d'informació fa que es sigui vulnerable davant les amenaces de seguretat. Així doncs, l'organització ha de fer un pas endavant en la gestió de la seguretat de la informació.

Per assolir aquest objectiu, cal seguir una metodologia per tal de reduir els riscos als quals està sotmesa l'organització. Existeixen varis estàndards que poden ajudar assolir aquest objectiu, com són NIST, NERC, ISO/IEC27001 ...

Des de l'organització es decideix apostar per la metodologia de la ISO (*International Organization for Standardization*) i en concret la ISO/IEC 27001 que específica els requisits per la implementació, el manteniment i la millora continua d'un sistema de Gestió de la seguretat de la informació, que és l'objectiu que es vol assolir.

Aquesta norma també inclou els requisits per l'apreciació i el tractament dels riscos de seguretat de la informació, seguint els requisits descrits a la Norma ISO/IEC 27001 [1] i fent ús d'eines, com pot ser, la Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes d'informació (MAGERIT) [5], que es veurà més endavant, podrem identificar i adoptar les mesures tècniques necessàries per corregir aquelles àrees més vulnerables i donar conformitat a la implementació d'un pla de seguretat en base a un estàndard internacional i tenint definit un procés de millora continua (PDCA).

Amb aquesta implementació aconseguirem tenir un mètode que ens donarà la seguretat de tenir un sistema implantat que doni confiança tant a l'organització com als col·lectius afectats, sabent que les seves dades estan protegides. Cal tenir en compte que el sector en què està la ONG els recursos són molt limitats, tot i que no he trobat una documentació especifica del tema, la implementació i

compliments del norma d'algun dels estàndards internacionals en les ONG's està molt per sota del que hauria. Creiem, per tant, que aquesta implementació ens donarà un tret diferencial cap a la resta de ONG's del sector, donant confiança tant a l'usuari com a l'administració.

En el cas que l'administració pública requerís dels serveis de l'organització per prestar aquest serveis essencials a col·lectius, l'organització es veuria obligada a donar compliment al Real Decret 311/2022 del 3 de maig, pel que es regula l'Esquema Nacional de Seguretat (ENS).

1.3 Enfocament i mètode seguit

El plantejament del projecte serà per tant, establir les bases d'un Pla director de seguretat per a l'empresa. Per simplificar, i com anirem veient, el nostre procés serà el següent:

- Analitzar i detallar el nostre inventari d'actius.
- Estudiar les amenaces a les que estem exposats.
- Estudiar l'impacte potencial de les mencionades amenaces.
- Proposar un pla d'acció per a lluitar contra aquestes amenaces.
- Avaluar l'impacte residual un cop aplicat el pla d'acció.

Intencionadament, la llista anterior no contempla aspectes organitzatius, encara que al llarg del projecte si que en parlarem d'aquests.

L'Organització ja ha anat fent processos de millora en alguns punts de la norma ISO/IEC 27001 [1], no obstant aquests no estan definits en un pla director de seguretat. Per aquest motiu, es recopilaran tots aquests treballs previs per tal d'unificar-los i encabir-los dins d'aquest pla director.

1.4 Planificació del Treball

La planificació del treball queda definida en el diagrama de Gantt de la figura 1. Com es pot observar està definit en 6 fases definides on al final de cadascuna d'elles comportarà l'inici de la següent, no obstant en cada fase posterior es revisarà i corregirà tot allò que faci falta de la fase anterior.

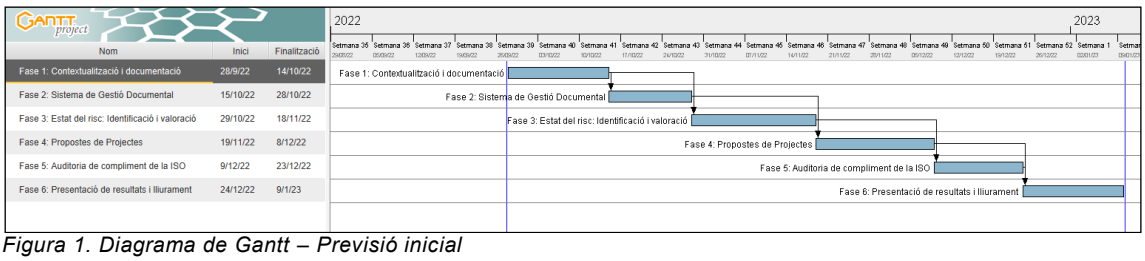

Figura 1. Diagrama de Gantt – Previsió inicial

Detallant, en cada fase buscarem els següents objectius:

Fase 1: Contextualització i documentació En aquesta primera fase es pretén indicar quin es el punt de partida de l'organització i quin és el context d'aquesta. Obtenint al final:

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

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

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

Fase 3: Estat del risc: Identificació i valoració En aquí es busca fer una identificació i valoració dels actius i amenaces a la que està sotmesa l'organització. Obtenint la següent documentació:

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

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

Fase 5: Auditoria de compliment de la ISO Informe d'auditoria de compliment de la ISO/IEC 27001.

Fase 6: Presentació de resultats i lliurament Consolidació dels resultats obtinguts, elaboració d'informes finals i presentació executiva a la direcció.

No obstant, per motius personals i aliens a la pròpia voluntat, aquesta planificació inicial ha quedat alterada i s'han hagut de comprimir i ajuntar fases, tal i com es pot observar en el segon diagrama de Gantt.

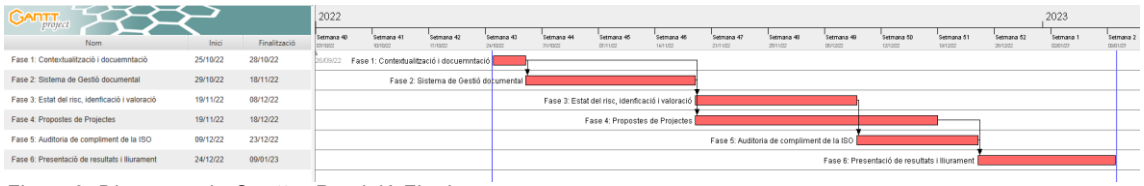

Figura 2. Diagrama de Gantt – Previsió Final

1.5 Breu sumari de productes obtinguts

En l'elaboració d'aquest treball s'ha pogut aprofundir en l'estat en que es troba l'organització en quant a seguretat de la informació. S'ha pogut constatar que tot i seguir una bona línia fins ara i veure que hi havia una bona pràctica en alguns sectors, sobretot s'havien realitzat inversions i s'havia posat èmfasi en infraestructura, també s'ha vist que alguns camps estaven mes descuidats, com poden ser en qüestions de conscienciació i formació.

Realitzar aquest treball, significa un pas més en aquest camp, adequar-se a la Norma ISO 27001, seguir un estàndard i elaborar tots els procediments que la norma implica a suposat una millora substancial en els resultats de l'organització.

Cal seguir treballant per aconseguir un nivell de maduresa òptim, que amb el pla de millora continuada implementat és factible arribar-hi en un període curt de temps.

1.6 Breu descripció dels altres capítols de la memòria

El treball ha estat estructurat per capítols i una sèrie d'annexos, que trobarem al final, en els capítols del treball es troba:

- Capítol 1 Introducció om es fa una breu descripció del treball.
- Capítol 2 Contextualització on es descriu l'organització i es marca l'abast en que es centrarà l'estudi d'aquest treball.
- Capítol 3 Sistema de Gestió documental on es farà un breu descripció de la documentació, anàlisis i procediments necessaris que s'han d'incloure en el treball i que es trobaran desenvolupats en els annexes.
- Capítol 4 Anàlisi de riscos sobre els actius de la organització.
- Capítol 5 Pla de projectes on es presenten una sèrie de projectes derivats de l'anàlisi de riscos fet en el capítol anterior.
- Capítol 6 Auditoria de compliment.
- Capítol 7 Conclusions extretes del present treball.
- Capítol 8 Glossari.
- Capítol 9 Referencies Bibliogràfiques.
- Capítol 10 a 16 Annexes amb la documentació descrita al capítol 3.
- Capítol 17 Anàlisi dels controls per l'auditoria de compliment.
- Capítol 18 Informe d'auditoria de compliment.

2. Contextualització i documentació

2.1 Descripció detallada de l'organització

L'organització que analitzaré en aquest TFM és una organització no governamental (ONG) que es dedica a l'atenció a les persones en diferents àmbits i a donar serveis essencials als seus usuaris. No es disposa d'una carta de serveis formals, ja que es tracte d'atendre a l'usuari en aquelles necessitats que es recull en cada moment, ja sigui per causes d'una pandèmia, d'una guerra, una crisi econòmica, etc. Està formada per unes 15000 persones entre treballadors i voluntaris que disposen d'usuari i correu electrònic, i que són els encarregats de donar el servei ja sigui als propis treballadors o voluntaris en l'àrea de secretaria o donar el servei a l'usuari final en l'àrea de coordinació.

L'ONG consta d'una seu central on s'ubica tota l'estructura de la organització i tots els seus departaments centrals. No obstant això, també disposa de 4 oficines Territorials, i unes 200 oficines locals distribuïdes pel territori per donar cobertura a aquests serveis essencials a nivell més local.

Tan la seu central, com les oficines territorials disposen d'un CPD on l'accés es fa mitjançant una targeta magnètica. La seu central és on s'ubica part dels serveis i bases de dades de la organització. Altre part es troba ubicada al núvol disposant d'un servei de O365. El CPD de la oficina central està redundat a un CPD d'un dels proveïdors de serveis de la organització. Els serveis de xarxa i comunicacions també es troben subcontractats a un proveïdor de serveis. Seguint el següent esquema:

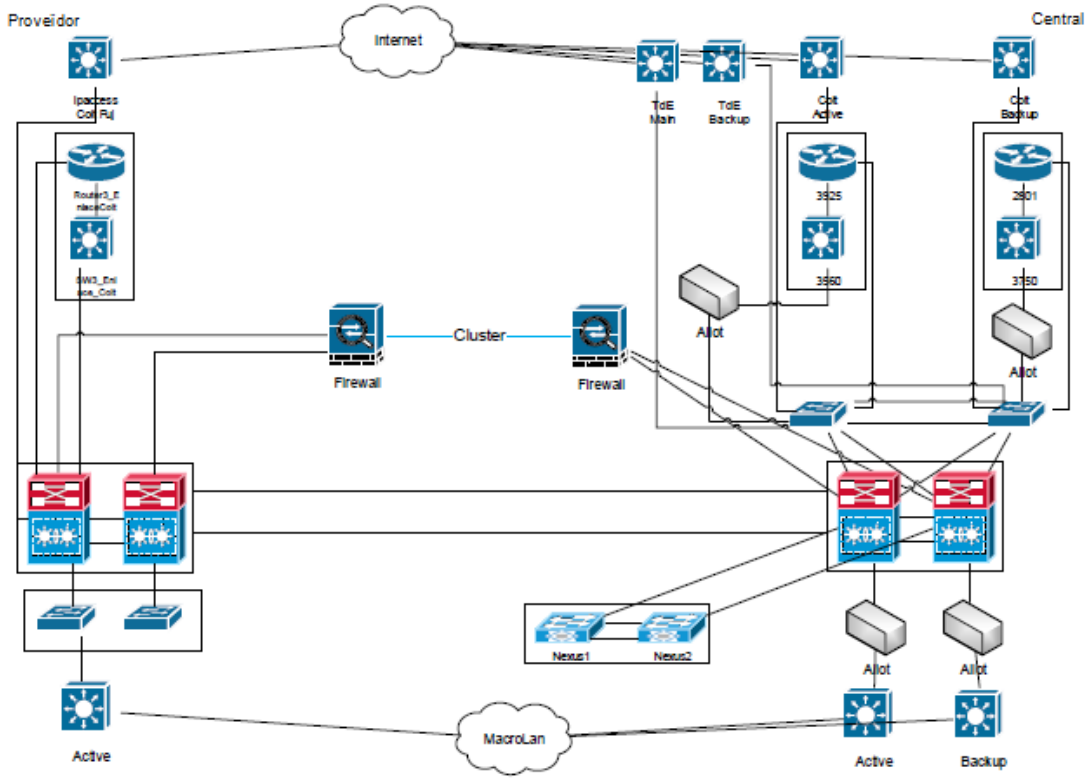

Figura 3. Mapa de connexions

Cap de les oficines disposa de seguretat ni control a les entrades, si que disposen de recepció, si que es disposen de càmeres de seguretat tant a la seu central com a les territorials, algunes de les oficines locals més petites també disposen de càmeres.

L'organigrama de la ONG segueix la següent estructura.

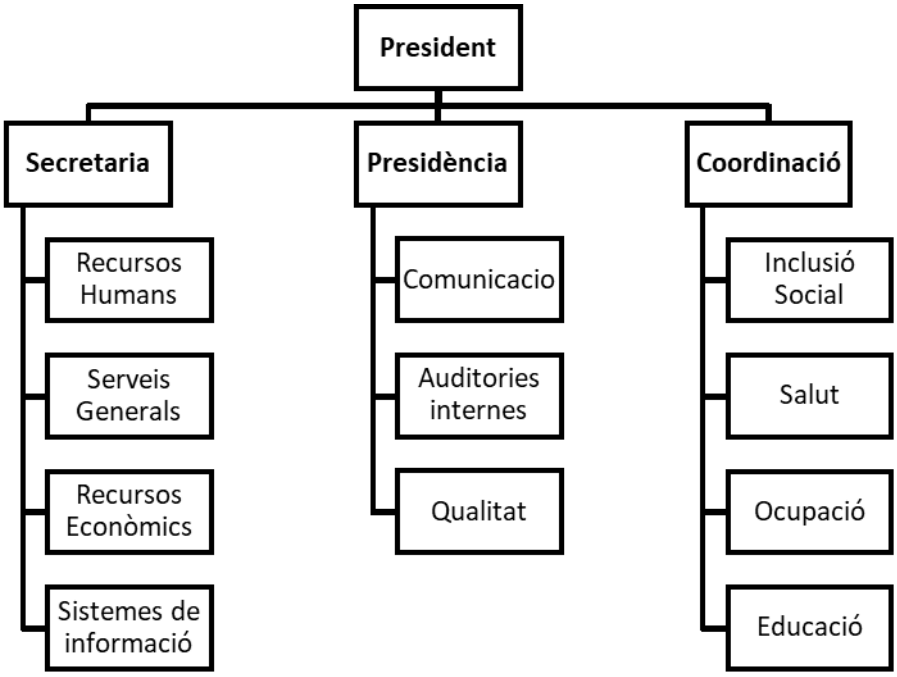

Figura 4. Organigrama

Dins d'aquesta estructura departamental cal indicar que hi ha tres nivells de funcionament. Local – territorial – Central, cadascun depenent del posterior.

L'inventari d'actius i el responsable d'aquests es troba definit a la següent Taula

Inventari d'actius			
Àmbit	**ID. Actiu**	**Actiu**	**Responsable**
Instal·lacions	L.1	Edificis	Director Serveis Generals
Instal·lacions	L.2	CPDs	CIO
Instal·lacions	L.3	Centre de Backup	CIO
Hardware	HW.1	Routers i Switchs	RSI
Hardware	HW.3	Firewalls	RSI
Hardware	HW.4	IDS/IPS	RSI
Hardware	HW.5	AP's	RSI
Hardware	HW.6	Servidors Producció	Responsable departament TID
Hardware	HW.7	Servidors Backup	Responsable departament TID
Hardware	HW.8	Servidors correu	Responsable departament TID
Hardware	HW.9	Entorn de proves	Responsable departament TID
Hardware	HW.10	Telèfons IP	Responsable departament TID
Hardware	HW.11	Telèfons mòbils	Responsable departament TID
Hardware	HW.12	Portàtils	Responsable departament TID
Hardware	HW.13	PC's usuari i ús genèric	Responsable departament TID
Hardware	HW.14	PC's accés públic	Responsable departament TID
Hardware	HW.15	Impressores	Responsable departament TID
Hardware	HW.16	Escàners	Responsable departament TID
Suports d'informació	MED.1	Cabina de discs (emmagatzematge de xarxa)	Responsable departament TID
Software	SW.1	Plataforma corporativa	Responsable departament TID
Software	SW.2	Gestor Base de Dades	Responsable departament TID
Software	SW.3	Office 365 corporatiu	Responsable departament TID
Software	SW.4	Antivirus	RSI
Software	SW.5	Sistemes operatius	Responsable departament TID

Dades	D.1	Fitxers personals	Treballador / Voluntari
Dades	D.2	Bases de dades Aplicacions	Responsable TID i DPO
Dades	D.3	Copies de Seguretat	Responsable TID i DPO
Dades	D.4	Bases de dades Gestió interna	Responsable TID i DPO
Dades	D.5	Dades control accés	Director SG i DPO
Dades	D.6	Codis font desenvolupament	Responsable TID i DPO
Dades	D.7	Registres	RSI i DPO
Dades	D.8	videovigilància	Director SG i DPO
Criptografia	KY.1	Certificats	DPO
Criptografia	KY.2	Claus d'encriptació portàtils	RSI
Xarxa	COM.1	Xarxa DMZ	RSI
Xarxa	COM.2	Accés Xarxa Pública	RSI
Xarxa	COM.3	Accés Xarxa Privada	RSI
Xarxa	COM.4	Xarxa Telefònica	RSI
Servei	S.1	Directori Actiu	Responsable TID
Servei	S.2	Web	Responsable TID
Servei	S.3	Serveis al usuari final	Directors de departament
Servei	S.4	VPN	RSI
Servei	S.5	Intranet	Responsable departament TID
Servei	S.6	O365 (correu i fitxers)	Responsable departament TID
Servei	S.7	Emmagatzematge de dades local	Responsable departament TID
Equipament auxiliar	AUX.1	Climatització	Director Serveis Generals
Equipament auxiliar	AUX.2	Control de portes	Director Serveis Generals
Equipament auxiliar	AUX.3	Càmeres Seguretat	Director Serveis Generals
Equipament auxiliar	AUX.4	SAI 's	Director Serveis Generals
Equipament auxiliar	AUX.5	Grup electrogen	Director Serveis Generals
Equipament auxiliar	AUX.6	Robot de cintes	Responsable departament TID
Equipament auxiliar	AUX.7	Mobiliari oficina	Director Serveis Generals
Personal	P.1	Administradors	CIO
Personal	P.2	Programadors	CIO
Personal	P.3	Treballadors	Director Recursos Humans
Personal	P.4	Voluntaris	Director Recursos Humans
Personal	P.5	Proveïdors	Director Serveis Generals

Taula 1. Inventari d'actius

S'ha realitzat un anàlisi de l'organització utilitzant l'anàlisi DAFO, que resumeix els aspectes claus de l'entorn de negoci i la capacitat estratègica. En aquest anàlisi s'analitzen les fortaleses i les debilitats i l'estudi de les amenaces i oportunitats.

	Punts forts	Punts dèbils
Origen Intern	**Fortaleses** La reputació de l'organització és alta, ja que és coneguda i valorada a nivell mundial Gran capacitat tècnica i humana per realitzar accions i activitats, l'organització està en constant creixement Gran transparència, al web es pot trobar tota la informació sobre el destí dels fons. Els Voluntaris i treballadors que tenen una gran dedicació i professionalitat Pla de Responsabilitat Social Corporativa Adaptació a les noves tecnologies Diferents fonts de finançament	**Debilitats** Finançament irregular Imatge tradicional que no afavoreix una participació dinàmica i juvenil del voluntariat Activitats molt diverses, això comporta que no s'identifiqui l'organització en un àmbit específic El gran número d'activitats dificulta la competitivitat i encareix els costos Comunicació deficient entre local-territori-central
Origen extern	**Oportunitats** La major conscienciació social de la població en els darrers temps Augment del voluntariat degut en gran part a la crisi econòmica. Millores en la comunicació i la informació sobre les necessitat. Major col·laboració d'empreses que volen ser responsables socialment Desgraciadament cada cop hi ha més demandes en el sector social que necessiten ser ateses	**Amenaces** La falta de transparència en alguns sectors del Tercer sector comporta una desconfiança generalitzada en organitzacions com la nostra Està augmentant la competència del sector lucratiu en les activitat del tercer sector portades a terme per ONGs L'augment del número d'ONGs comporta un menor finançament ja que les aportacions col·laboratives estan més diversificades Manca de publicitat en les activitats i ajudes que es porten a terme des de l'organització La crisi econòmica ha comportat una reducció dels pressupostos degut a la manca de finançament

Figura 5. Anàlisi DAFO

2.2 Abast del pla director

L'abast del Pla Director de Seguretat (PDS) es centrarà en totes les àrees de l'organització, incloent els centres territorials i/o locals des d'on s'ofereixen serveis essencials. Recollir l'estat actual dels nivells de seguretat i els actius que tenen relació directa amb els sistemes de informació en els processos en que es dona serveis als usuaris.

Establir els criteris de control apropiats per ser efectius, eficients, aconseguint confidencialitat i integritat i complir amb les exigències del Reglament (UE) 2016/679 i la Llei Orgànica 3/2018. Així com, tenir la base per avançar cap al compliment de les mesures de seguretat fixades a l'Esquema Nacional de Seguretat (ENS), en el cas que aquestes serveis essencials siguin per encàrrec de l'administració pública.

2.3 Anàlisi diferencial de compliment inicial i presentació de resultats

Abans de començar amb el projecte d'implantació cal realitzar un anàlisis del compliment inicial de les mesures de seguretat que requereix la normativa de la ISO/IEC 27001:2017 i posteriorment el compliment dels controls definits en aquesta mateixa i desenvolupats a la ISO/IEC 27002:2017. Aquesta valoració es realitza segons la següent taula, que es basa en el Model de Maduresa de la Capacitat (CMM):

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

Taula 2. Model de Maduresa de la Capacitat (CMM)

Tal i com s'observa a la taula, aquest valoració la podem realitzar tant utilitzant el valor definit a la columna efectivitat utilitzant el %, o utilitzant un valor numèric definit entre 0 i 5 tal i com està definit a la columna CMM.

En la taula següent es valora el nivell de compliment actual de la norma ISO/IEC 27001:2017

Secció	Requeriment	Descripció	Subnivell de compliment	Nivell de compliment	Nivell objectiu	Justificació
4	Context de l'organització			**1,75**	**3**	
4.1	Comprensió de la organització i el seu context			**2,00**		Existeixen procediments de seguretat, però no es té cap política detallada i aprovada per l'organització que defineixi l'abast i els objectius a nivell institucional. Existeixen una sèrie de normatives com poden ser: La normativa de protecció de dades, ús dels equips, ús del correu electrònic, guies de protecció de dades, guies d'orientació sobre l'ús de missatgeria com per exemple whatsapp. Procediment de l'exercici del dret. Els procediments existents estan dirigits bàsicament el compliment de la protecció de dades. Es troben establerts procediments de Seguretat com: Pla de manteniment, pla de proves, pla de seguiment i control de les millores indicades, seguiment de incidents, gestió de crisis, llistat de procediments per servei, alta i baixa d'usuaris, procediment i programació de copies de seguretat, guia per administradors territorials de SI, procediment formalitzat per la gestió d'incidències, Pla director de seguretat.
		Estan identificats els objectius del SGS Sistema de Gestió de la Seguretat de la Informació?	2			
		S'han identificat les qüestions internes i externes relacionades amb la seguretat de la informació?	2			
		S'han identificat com les parts internes i externes poden suposar amenaces o riscos per a la seguretat de la informació?	2			
4.2	Comprensió de les necessitats i expectatives de les parts interessades			**3,00**		
		S'han identificat les parts interessades?	3			
		Hi ha un llistat de requisits sobre Seguretat de la Informació de les parts interessades?	3			
		Hi ha un llistat de requisits sobre Seguretat de la Informació referent a reglaments, requisits legals i requisits contractuals?	3			
4.3	Determinació de l'abast del SGSI			**1,00**		
		S'ha determinat l'abast del SGSI i se'n conserva informació documentada?	1			
4.4	Sistema de gestió del SGSI			**1,00**		
		El sistema de Gestió de Seguretat de la informació SGSI està establert, implementat i es revisa de manera planificada considerant oportunitats de millora?	1			
5	Lideratge			**2,11**	**3**	
5.1	Lideratge i compromís			**2,33**		La justificació es la mateixa que es troba explicada en la secció 4

		S'han establert objectius de la Seguretat de la Informació d'acord amb els objectius del negoci?	2			
		La direcció proveeix dels recursos materials i humans necessaris per al compliment dels objectius del SGSI?	3			
		La direcció revisa directament l'eficàcia de l'SGSI per garantir que es compleixen els objectius de l'SGSI?	2			
5.2	Política			**1,00**		
		S'ha definit una política de seguretat de la informació?	1			
		S'ha establert un marc que permeti establir objectius?	1			
		S'ha comunicat la política de seguretat de la informació a les parts interessades i a tota l'empresa?	1			
		Es manté informació documentada de la política de l'SGSI i dels seus objectius?	1			
5.3	Rols i Responsabilitats			**3,00**		
		S'han assignat les responsabilitats i les autoritats sobre la Seguretat de la Informació?	3			
		S'han comunicat convenientment les responsabilitats i les autoritats per a la Seguretat de la Informació?	3			
6	Planificació			**1,60**	**3**	
6.1	Tractament de Riscos i Oportunitats			**1,20**		Està pendent la realització d'un anàlisis de risc, en el què s'avaluïn tots els actius implicats en el tractament de la informació, i l'establiment d'un pla pel tractament del risc. Es realitzen tractaments amb mesures de control insuficients en centres territorials i locals que incorporen riscos en el sistema
		El pla per abordar riscos i oportunitats considera les expectatives de les parts interessades en relació amb la seguretat de la informació?	2			
		S'identifiquen i analitzen els riscos mitjançant un mètode d'avaluació i d'acceptació de riscos?	1			
		S´ha definit un procés de tractament de riscos?	1			

		S'han establert criteris per elaborar una declaració d'aplicabilitat?	1			
		Es manté informació documentada dels punts anteriors?	1			
6.2	Planificació per aconseguir objectius			**2,00**		
		S'han establert objectius de la Seguretat de la Informació mesurables i d'acord amb els objectius del negoci?	2			
		Els objectius de la Seguretat de la Informació estan planificats mitjançant? -Assignació de responsabilitats -Cronograma d'execució temporal -Mètode devaluació	2			
		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?	2			
7	Suport			**2,73**	**4**	
7.1	Recursos			**2,00**		En línia del valorat a les seccions 4 i 5.
		S'identifiquen i assignen els recursos necessaris per a l'SGSI?	2			
7.2	Competència			**3,00**		S'han realitzat formacions al personal i s'estableixen plans de formació tots els anys. En centres territorials i locals s'han detectat deficiències (sobretot en l'ús de dispositius d'emmagatzematge i transferència de fitxers per correu i altres.
		S'avalua la competència en matèries de seguretat de la informació per a persones que efectuen tasques que puguin afectar la seguretat?	3			
		Es manté informació actualitzada sobre la competència del personal?	3			
7.3	Conscienciació			**3,00**		S'han realitzat accions formatives i guies pel personal. Aquest coneix els procediments per l'exercici dels drets i informar de les bretxes de seguretat.
		El personal està involucrat i és conscient del seu paper a la Seguretat de la Informació?	3			
		Hi ha consciència dels danys que es poden produir de no seguir les pautes de la Seguretat de la Informació?	3			

				3,00		
7.4	Comunicació	Es comunica la política de la Seguretat de la Informació amb les responsabilitats de cadascú?	3			El personal coneix procediments per informar de bretxes de seguretat i l'exercici de drets
		Hi ha un procés per comunicar les deficiències o males pràctiques en la seguretat de la informació?	3			
				2,67		
7.5	Informació Documentada	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.)	2			La documentació i procediments es troben comentats a la secció 4.
		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	3			
		Es controlen els documents d'origen extern?	3			
8	Operació			**1,33**	**3**	
				2,00		Està pendent la realització d'un anàlisis de risc, en el què s'avaluïn tots els actius implicats en el tractament de la informació, i l'establiment d'un pla pel tractament del risc. Es realitzen tractaments amb mesures de control insuficients en centres territorials i locals que incorporen riscos en el sistema. Tot i que existeixen procediments en relació a la seguretat
8.1	Control Operacional	Els processos de seguretat de la informació estan documentats per controlar que es realitzen segons el planificat?	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			

		S'estableixen mesures i plans per mitigar els riscos a la Seguretat de la Informació davant de canvis realitzats?	2			tal i com hem indicat en seccions anteriors.
		S'identifiquen i es controlen els processos externalitats quant als riscos per a la Seguretat de la Informació?	2			
8.2	Anàlisi de riscos de la Seguretat de la Informació			**1,00**		
		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	1			
8.3	Tractament de riscos de la Seguretat de la Informació			**1,00**		
		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	1			
		S'identifiquen tots els controls necessaris per mitigar el risc justificant-ne l'aplicació?	1			
		Es documenta el nivell d'aplicació de tots els controls que cal aplicar?	1			
9	Avaluació de l'exercici			**2,78**	**4**	
9.1	Seguiment i mesurament			**3,00**		Existeix un catàleg d'amenaces i vulnerabilitats en el que s'estableixen indicadors per mesurar els nivells dels riscos, probabilitats i impactes sobre el sistema. No obstant, no estan recolzats per l'anàlisi de riscos pertinent, per mesurar les salvaguardes i els nivells de seguretat. El sistema de mètrica ha d'evolucionar.
		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?	3			
		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?	3			

9.2	Auditories Internes			**2,33**		s'han realitzat auditories externes per saber el nivell de seguretat i S'estableixen unes recomanacions per establir un pla director de seguretat on s'estableixin un pla d'auditories internes
		S'ha establert una programació d'auditories internes i assignat responsables?	3			
		L'abast i els requisits s'han definit per a l'informe d'auditoria?	2			
		Es consideren accions correctives i propostes de canvi als informes d'auditoria?	2			
9.3	Informe de Revisió per la Direcció			**3,00**		Existeix un comitè de seguretat que s'encarrega de realitzar aquesta tasca.
		Hi ha una programació per als informes de la direcció i hi ha constància de la seva realització periòdica?	3			
		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?	3			
10	Millora			**2,25**	**4**	
10.1	No Conformitats i accions correctives			**2,50**		En la línia del que s'ha descrit en les seccions anteriors
		Hi ha un procediment documentat per identificar i registrar les no-conformitats i el seu tractament?	3			
		Dins de les accions correctives hi ha una diferenciació entre accions correctives sobre la no-conformitat i sobre les causes de la mateixa?	2			
10.2	Millora continua			**2,00**		
		Hi ha un procés per garantir la millora contínua de l'SGSI identificant les oportunitats de millora?	2			

Taula 3. Anàlisi de compliment inicial de la Norma ISO 27001

Els valors que podem observar a la taula 2 es basen en el fet que l'ONG ha decidit implementar la norma ISO/IEC 27001 en els seus processos, tot i que hi ha molts processos definits i polítiques desenvolupades s'han de millorar, revisar i actualitzar i recollir en una política de seguretat que no està desenvolupada.

Per aquest motiu, s'ha designat un equip per liderar i portar a terme la implementació d'un SGSI, un pla de seguretat que permeti consolidar la

organització al cap davant del sector, per aquest motiu es dotarà a l'equip dels recursos necessaris per tal efecte.

En aquests moments s'està realitzant la recol·lecció de tota la documentació i treballs que s'han realitzat de forma independent.

Com es veu clarament a la aquesta figura 6, l'estat d'implementació inicial està en un estat de maduresa en que es veu que encara falta definir molts aspectes i una mica lluny dels objectius desitjables.

En aquest gràfic podem observar els resultats obtinguts en la valoració inicial del compliment de la norma ISO/IEC 27001.

La línia vermella ens indica l'estat actual del compliment de la norma.

L'objectiu que es busca és el de tenir tots els controls siguin gestionats i es puguin mesurar que seria la línia groga.

En verd trobem l'estat de compliment òptim de la norma

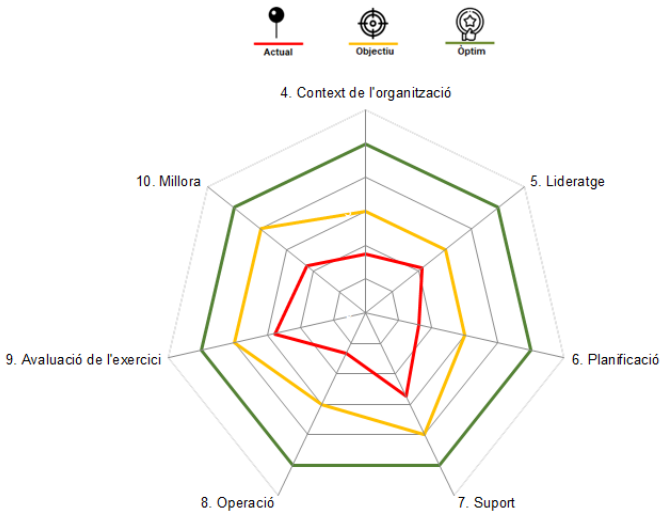

Figura 6. Anàlisi inicial GAP de la Norma

En aquesta altre figura podem veure com es reparteix l'estat de maduresa dels requeriments on bona part d'aquest s'ha treballat amb ells de forma individual però falta acabar de definir el procés.

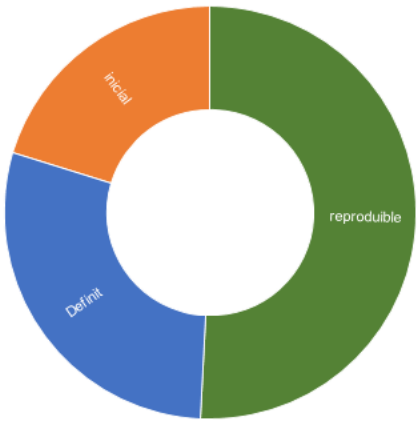

Figura 7. Nivells de Maduresa de la norma

En aquesta altre taula es valora el nivell de compliment actual dels controls que es troben a l'Annex A de la ISO/IEC 27001:2017 i que es desenvolupen a la ISO/IEC 27002:2017.

Secció	Requeriment	Descripció	Subnivell de compliment	Nivell de compliment	Nivell objectiu	Justificació
A.5	Polítiques de seguretat de la informació			**2,00**	**4**	
A.5.1	Directrius de gestió de la seguretat de la informació			**2,00**		Existeixen una sèrie de normatives com poden ser: La normativa de protecció de dades, ús dels equips, ús del correu electrònic, guies de protecció de dades, guies d'orientació sobre l'ús de missatgeria com per exemple whatsapp. Procediment de l'exercici del dret.
		Polítiques per a la seguretat de la informació	2			
		Revisió de les polítiques per a la seguretat de la informació	2			
A.6	Organització de la Seguretat de la informació			**2,55**	**4**	
A.6.1	Organització interna			**2,60**		
		Rols i responsabilitats en seguretat de la informació.	3			Estan definits rols i les responsabilitats però no dins d'un pla global.
		Segregació de tasques.	3			En la gestió dels rols i responsabilitats també existeix un protocol de segregació de tasques
		Contacte amb les autoritats.	3			Existeix un procediment de notificació de bretxes de seguretat
		Contacte amb grups d' interès especial.	2			No existeix un procediment específic per aquest tipus de contacte amb grups especials
		Seguretat de la informació en la gestió de projectes.	2			No existeix un procediment específic per la seguretat en la gestió de projectes
A.6.2	Els dispositius mòbils i el teletreball.			**2,50**		
		Política de dispositius mòbils.	2			No hi ha una guia específica sobre mòbils, però si sobre missatgeria.
		Teletreball.	3			Existeix una guia sobre Teletreball
A.7	Seguretat relativa als recursos humans			**2,83**	**3**	
A.7.1	Abans de l' ocupació.			**2,50**		
		Investigació d' antecedents.	2			Es fa aquesta investigació a les persones que treballen amb menors. La resta no es fa.
		Termes i condicions de l' ocupació.	3			Es tenen polítiques internes i acords de confidencialitat i normatives de protecció de dades
A.7.2	Durant l' ocupació.			**3,00**		
		Responsabilitats de gestió.	3			Es tenen polítiques internes i acords de confidencialitat i normatives de protecció de dades

		Conscienciació, educació i capacitació en seguretat de la informació.	3			Es realitzen accions formatives i guies pel personal, tot i que s'han detectat moltes deficiències
		Procés disciplinari.	3			Estan incloses en les polítiques internes de l'organització
A.7.3	Finalització de l' ocupació o canvi de lloc de treball.			**3,00**		
		Responsabilitat davant la finalització o canvi.	3			Estan inclosos en els acords de confidencialitat
A.8	Gestió d'actius			**2,19**	**4**	
A.8.1	Responsabilitat sobre els actius.			**2,25**		
		Inventari d' actius.	2			L'inventari existent només està referit als equips informàtics, ordinadors i servidors, però no la resta d'actius.
		Propietat dels actius.	2			Existeix una assignació en els actius inventariats, però amb bastantes deficiències
		Ús acceptable dels actius.	3			Existeix una normativa sobre l'ús dels equips
		Devolució d' actius.	2			Està inclosa en la normativa d'ús dels actius, però amb deficiències
A.8.2	Classificació de la informació.			**1,67**		
		Classificació de la informació.	1			La informació que afecte a dades personals es troba recollida en un registre d'activitats del tractament, però no existeix cap altre tipus de classificació
		Etiquetatge de la informació.	2			Els suports de dades s'etiqueten per la conservació i custodia, però cal un procediment
		Manipulat de la informació.	2			Existeix un procediment d'alta i baixa d'usuaris a les aplicacions, però cal ampliar i millorar
A.8.3	Manipulació dels suports.			**2,67**		
		Gestió de suports extraïbles.	2			Existeix una guia de recomanacions i bones pràctiques on es recull el xifrat de dades i emmagatzemament de suports extraïbles, però existeixen deficiències.
		Eliminació de suports.	3			Existeix un procediment establert per la destrucció d'equips informàtics i esborrat i destrucció de suports de dades. En el cas de mitjans no electrònics es fa ús de destructores. Tot i que s'ha detectat alguna deficiència
		Suports físics en trànsit.	3			Els suports de copies de seguretat són enviats fora a un proveïdor extern
A.9	Control d'accés			**2,87**	**4**	

A.9.1	Requisits de negoci per al control d' accés.			**3,00**		
		Polítiques de control d' accés	3			Es disposa d'un procediment de gestió d'altes d'usuari, els permisos són assignats en correspondència a les funcions a realitzar
		Accés a les xarxes i als serveis de xarxa.	3			
A.9.2	Gestió d' accés d' usuari.			**2,67**		
		Registre i baixa d' usuari	2			Els usuaris queden identificats en polítiques a través de directori actiu, polítiques a través de les plataformes d'aplicacions i de correu O365. No obstant hi ha deficiències en la comunicació de les baixes d'usuaris
		Provisió d' accés d' usuari.	3			Es defineix una política de mínim privilegi, que permet que els usuaris tinguin accés als recursos pel desenvolupament de les seves activitats, també es disposa del procediment d'alta d'usuari
		Gestió de privilegis d' accés.	3			
		Gestió de la informació secreta d' autenticació dels usuaris.	3			S'estableixen restriccions per l'ús de les claus de seguretat i directives de contrasenyes en el directori actiu, aplicacions i correu. No es permet l'ús compartit de claus d'accés.
		Revisió dels drets d' accés d' usuari.	3			S'estableixen caducitats en les claus d'accés, però existeix una deficiència de comunicació de baixes d'usuari també es detecta falta de comunicació en la revisió i retirada de drets d'accés
		Retirada o reassignació dels drets d' accés.	2			
A.9.3	Responsabilitat de l' usuari.			**3,00**		
		Ús de la informació secreta d' autenticació.	3			S'estableixen restriccions per l'ús de les claus de seguretat i directives de contrasenyes en el directori actiu, aplicacions i correu. No es permet l'ús compartit de claus d'accés.
A.9.4	Control d' accés a sistemes i aplicacions.			**2,80**		
		Restricció de l'accés a la informació.	3			Els permisos són assignats en correspondència a les funcions a realitzar
		Procediments segurs d' inici de sessió.	3			S'estableixen restriccions per l'ús de les claus de seguretat i directives de contrasenyes en el directori actiu, aplicacions i correu. No es permet l'ús compartit de claus d'accés, també s'incorporen pantalles informatives on s'accepten les condicions de privacitat
		Sistemes de gestió de contrasenyes.	3			S'estableixen restriccions per l'ús de les claus de seguretat i directives de contrasenyes en el directori actiu, aplicacions i correu

		Ús d' utilitats amb privilegis del sistema.	3			Els permisos són assignats en correspondència a les funcions a realitzar
		Control d' accés al codi font dels programes.	2			Els desenvolupaments es realitzen sobre una plataforma de desenvolupament aplicant metodologies conegudes. Tot i que s'han detectat aplicacions en centres territorials i locals fora d'aquest control
A.10	Criptografía			**2,00**	**3**	
A.10.1	Controls criptogràfics.			**2,00**		
		Polítiques d' ús dels controls criptogràfics.	3			Xarxes i clients VPN per les connexions remotes. Plataformes web amb xifrat de les comunicacions. Existeix una normativa de recomanacions i bones pràctiques que recull l'enviament de documents xifrats o protegits amb claus d'accés a través de correu electrònic. Les copies de seguretat també estan xifrades
		Gestió de Claus	1			No existeix cap procediment al respecte
A.11	Seguretat física i de l'entorn			**2,72**	**4**	
A.11.1	Àrees segures.			**3,00**		
		Perímetre de seguretat física.	3			Existeixen varis CPDs amb control d'accés, també arxius amb informació confidencial amb control d'accés, tancats i amb climatització pròpia es disposa de càmeres de seguretat en els centres amb gravació d'imatge
		Controls físics d' entrada.	3			
		Seguretat d' oficines, despatxos i recursos.	3			
		Protecció contra les amenaces externes i ambientals.	3			
		El treball en àrees segures.	3			
		Àrees de càrrega i descàrrega.	3			Es disposa de càmeres de seguretat en els centres amb gravació d'imatge
A.11.2	Seguretat dels equips.			**2,44**		
		Emplaçament i protecció d' equips.	2			Els CPDs estan ubicats en locals independents amb accés controlat en la seu central i territorial, però no sempre succeeix en els centre locals.
		Instal·lacions de subministrament.	3			Els CPD's disposen de SAI i climatització redundada, les oficines locals disposen de SAI per l'armari rack però no tots els centres disposen de SAI per la resta d'equips.

		Seguretat del cablejat.	2			Els CPDs estan ubicats en locals independents amb accés controlat en la seu central i territorial, però no sempre succeeix en els centre locals.
		Manteniment dels equips.	2			Es preparen els equips amb una maqueta aprovada pel departament de Sistemes, aplicant les mesures de seguretat pertinent. Es disposen de servidors d'actualitzacions per minimitzar riscos. Però es detecten deficiències.
		Retirada de materials de l' empresa.	3			Existeix un inventari d'equips i una política de renovació i retirada dels equips. Però existeixen algunes deficiències
		Seguretat dels equips fora de les instal·lacions.	2			Existeix l'inventari i l'assignació de l'actiu, però no es fa un seguiment dels equips
		Reutilització o eliminació segura d' equips.	3			Existeix un procediment establert per la destrucció d'equips informàtics i esborrat i destrucció de suports de dades
		Equip d' usuari desatès.	3			Existeix una política per inactivitat a través de polítiques de domini.
		Política de lloc de treball ordenat i pantalla neta.	2			El personal coneix la política de lloc de treball net. Però existeixen moltes deficiències i no es fa un seguiment correcte
A.12	Seguretat de les operacions			**2,57**	**4**	
				2,50		
A.12.1	Requisits de negoci per al control d' accés.	Documentació de procediments operacionals.	3			S'han establert diferents procediments de seguretat com poden ser el pla de manteniment, pla de proves, pla de seguiment i control de millores, seguiment d'incidents, gestió de crisis, llistats de procediments per serveis, alta i baixa d'usuaris, procediments de copies de seguretat, guia d'administradors territorials de si i procediment de gestió d'incidències
		Gestió de canvis.	2			Es preparen els equips amb una maqueta aprovada pel departament de Sistemes, aplicant les mesures de seguretat pertinent per disminuir el risc; tot i que existeixen deficiències en alguns centres.
		Gestió de capacitats.	2			La direcció i l'àrea de SI decideixen les necessitats dels nous components en funció dels volums de dades i la qualitat dels serveis. Hi ha un pla de contingències que inclou un pla de proves, seguiment i millores. S'han incorporat mesures per evitar atacs de denegació de servei.

		Separació dels recursos de desenvolupament, prova i operació.	3			Existeixen procediments on es recullen les etapes d'implementació i posada en producció dels softwares desenvolupats per l'organització, les proves es realitzen en entorns aïllats i segurs
A.12.2	Protecció contra el programari maliciós (malware).			**2,00**		
		Controls contra el codi maliciós.	2			El departament de sistemes i els responsables de seguretat instal·len i gestionen els antivirus als equips i servidors i verifiquen l'actualització periòdica. S'han detectat deficiències en alguns territoris
A.12.3	Còpies de seguretat de la informació.			**3,00**		
		Còpies de seguretat de la informació.	3			Es realitzen copies de seguretat encriptades seguint el procediment de copies de seguretat. Es realitzen copies de seguretat sistemàtiques en tots els CPDs. A més el CPD de la oficina central es un CPD d'alta disponibilitat Actiu-Actiu
A.12.4	Registres i supervisió.			**3,00**		
		Registres d' esdeveniments.	3			Està activat el control de logs tant en servidors com en aplicacions corporatives. Es realitzen anàlisis periòdics per detectar incidències de seguretat. També es disposa de sistemes de detecció d'intrusions (IDS/IPS).
		Protecció de la informació del registre.	3			Els registres d'activitat estan protegits i només estan accessibles pels responsables de seguretat
		Registres d' administració i operació.	3			Està activat el control de logs tant en servidors com en aplicacions corporatives. Es realitzen anàlisis periòdics per detectar incidències de seguretat. També es disposa de sistemes de detecció d'intrusions (IDS/IPS).
		Sincronització del rellotge.	3			Els equips i servidors estan sincronitzats a una únic servidor.
A.12.5	Control del programari en explotació.			**3,00**		
		Instal·lació del programari en explotació.	3			Existeixen procediments on es recullen les etapes d'implementació i posada en producció dels softwares desenvolupats per l'organització, les proves es realitzen en entorns aïllats i segurs
A.12.6	Gestió de la vulnerabilitat tècnica.			**2,50**		

		Gestió de les vulnerabilitats tècniques.	3			Existeixen procediments on es recullen les etapes d'implementació i posada en producció dels softwares desenvolupats per l'organització, les proves es realitzen en entorns aïllats i segurs
		Restricció en la instal·lació del programari.	2			La instal·lació està restringida per defecte en el procediment d'alta i baixa d'usuaris.
A.12.7	Consideracions sobre l' auditoria de sistemes d' informació.			**2,00**		
		Controls d' auditoria de sistemes d' informació.	2			S'han realitzat auditories de seguretat externes per saber l'estat de seguretat del sistema i les aplicacions.
A.13	Seguretat de les comunicacions			**3,17**	**4**	
A.13.1	Gestió de la seguretat de les xarxes.			**3,33**		
		Controls de xarxa.	3			Procediment d'alta i baixa d'usuaris a les aplicacions; Punts d'accés a internet amb internet d'alta disponibilitat, Firewall, control del tràfic e/s, identificació de ports i serveis necessaris. El nivell de maduresa del CPD central és alt, però hi ha deficiències en altres CPDs territorials. Utilització de xarxes i canals VPN per les connexions exteriors. Plataformes web amb xifrat de comunicacions. Separació de les xarxes de producció i desenvolupament i la xarxa DMZ per serveis externs mitjançant dispositius de Firewall
		Seguretat dels serveis de xarxa.	3			
		Segregació en xarxes.	4			
A.13.2	Intercanvi d' informació.			**3,00**		
		Polítiques i procediments d' intercanvi d' informació.	2			Polítiques i procediments descrits en tots els punts anteriors que recullen parts dels procediments, però no existeix un específic només aquest procediment
		Acords d' intercanvi d' informació.	3			S'incorporen als contractes amb proveïdors l'abast dels serveis. Es tenen documentats els serveis contractats amb els nivells de disponibilitat i persones de contacte.
		Missatgeria electrònica.	4			Correu corporatiu O365 gestionat pel departament de sistemes central amb mesures anti-spam i anti-malware. Existeix una normativa d'ús del correu electrònics i procediments d'enviament de documentació adjunta.
		Acords de confidencialitat o no revelació.	3			Es tenen polítiques internes i acords de confidencialitat i normatives de protecció de dades
A.14	Adquisició, desenvolupament i manteniment dels sistemes d'informació			**2,78**	**4**	

				2,67		
		Anàlisi de requisits i especificacions de seguretat de la informació.	2			La direcció i l'àrea de sistemes decideixen les necessitats dels nous components
A.14.1	Requisits de seguretat en els sistemes d' informació.	Assegurar els serveis d' aplicacions en xarxes públiques.	3			Plataformes web amb xifrat de comunicacions. Separació de les xarxes de producció i desenvolupament i la xarxa DMZ per serveis externs mitjançant dispositius de Firewall
		Protecció de les transaccions de serveis d' aplicacions.	3			Es disposa d'un repositori de certificats a Azure que permet la datació del temps
				2,67		
		Política de desenvolupament segur.	2			Els desenvolupaments es realitzen sobre una plataforma de desenvolupament aplicant metodologies conegudes. Si tracten dades de caràcter personal es sotmeten a avaluació de l'impacte a la privacitat. Es realitzen auditories de seguretat per conèixer les possibles vulnerabilitats i vectors d'atac per prevenir incidents de seguretat. Tot i que s'han detectat aplicacions en centres territorials i locals fora d'aquest control
		Procediment de control de canvis en sistemes.	2			Es preparen els equips amb una maqueta aprovada pel departament de Sistemes, aplicant les mesures de seguretat pertinent per disminuir el risc; Es disposen de servidors d'actualitzacions per minimitzar riscos tot i que existeixen deficiències en alguns centres.
A.14.2	Seguretat en el desenvolupament i en els processos de suport.	Revisió tècnica de les aplicacions després d' efectuar canvis en el sistema operatiu.	2			
		Restriccions als canvis en els paquets de programari.	3			s defineix una política de mínim privilegi, que permet que els usuaris tinguin accés als recursos pel desenvolupament de les seves activitats, però no realitzar canvis en el programari
		Principis d' enginyeria de sistemes segurs.	3			Es realitzen actualitzacions de seguretat i control de ports i serveis.
		Entorn de desenvolupament segur.	3			Descrit en el punt 14.2.1
		Externalització del desenvolupament de programari.	3			El desenvolupament de programari propi és intern i està subjecte al descrit en punts anteriors, en cas que s'externalitzés hauria de seguir els procediments establerts per l'organització
		Proves funcionals de seguretat de sistemes.	3			Es té un procediment on es recullen les etapes d'implementació i la posada en producció del softwares desenvolupats, i les proves es realitzen en entorns aïllats i segures
		Proves d' acceptació de sistemes.	3			

A.14.3	Dades de prova.			**3,00**		
		Protecció de les dades de prova.	3			Queden protegides per la plataforma de desenvolupament.
A.15	Relació amb proveïdors			**3,00**	**4**	
A.15.1	Seguretat en les relacions amb proveïdors.			**3,00**		
		Política de seguretat de la informació en les relacions amb els proveïdors.	3			S'incorpora en els contractes amb els proveïdors l'abast dels serveis i es disposa d'un document amb els serveis contractats amb els nivells de disponibilitat i les persones de contacte.
		Requisits de seguretat en contractes amb tercers.	3			
		Cadena de subministrament de tecnologia de la informació i de les comunicacions.	3			
A.15.2	Gestió de la provisió de serveis del proveïdor.			**3,00**		
		Control i revisió de la provisió de serveis del proveïdor.	3			El departament de sistemes és l'encarregat de vetllar pel correcte funcionament diari dels serveis i establir els mecanismes de control
		Gestió de canvis en la provisió del servei del proveïdor.	3			
A.16	Gestió d'incidents de seguretat de la informació			**2,86**	**4**	
A.16.1	Gestió d' incidents de seguretat de la informació i millores.			**2,86**		
		Responsabilitats i procediments.	2			Existeix un procediment de notificació de bretxes i un procediment d'exercici de drets.
		Notificació dels esdeveniments de seguretat de la informació.	3			L'àrea de sistemes gestiona els incident de seguretat i posa en funcionament les mesures necessàries per la resolució. Es disposa d'una aplicació pel registre de les incidències i s'assignen les incidències a persones responsables per donar resposta i es manté un control i seguiment
		Notificació de punts febles de la seguretat.	3			
		Avaluació i decisió sobre els esdeveniments de seguretat d' informació.	3			
		Resposta a incidents de seguretat de la informació.	3			
		Aprenentatge dels incidents de seguretat de la informació.	3			
		Recopilació d' evidències.	3			
A.17	Aspectes de seguretat de la informació per la gestió de la continuïtat del negoci			**3,17**	**4**	
A.17.1				**2,33**		

	Continuïtat de la seguretat de la informació.	Planificació de la continuïtat de la seguretat de la informació.	1			Es té definit un pla de contingència tecnològica o s'incorporen rols i responsabilitats dins del pla, seguiment i continuïtat dels serveis amb el seu corresponent pla de proves, control i seguiment. Però manca un anàlisi d'impacte
		Implementar la continuïtat de la seguretat de la informació.	3			
		Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	3			
A.17.2	Redundàncies.			**4,00**		
		Disponibilitat dels recursos de tractament de la informació.	4			Es disposa d'un CPD en modalitat Actiu-Actiu en alta disponibilitat. Es garanteix la disponibilitat de persones que realitzaran les tasques essencials en cas de falta del personal habitual. Generalment es disposa de mitjans alternatius per la substitució d'equips en cas de fallada. Totes les comunicacions estan redundades
A.18	Compliment			**2,20**	**4**	
A.18.1	Compliment dels requisits legals i contractuals.			**2,40**		
		Identificació de la legislació aplicable i dels requisits contractuals.	1			Existeixen procediments de de seguretat però no es té una política de seguretat detallada i aprovada per l'organització
		Drets de Propietat Intel·lectual (DPI).	2			
		Protecció dels registres de l' organització.	2			
		Protecció i privacitat de la informació de caràcter personal.	4			S'han identificat els tractament de dades personals al sistema i es realitzen auditories de protecció de forma periòdica.
		Regulació dels controls criptogràfics.	3			Existeix el repositori de certificats, Les copies de seguretat estan xifrades, la transferència de dades a l'exterior també estan xifrades, (vpn-https).
A.18.2	Revisió independent de la seguretat de la informació.			**2,00**		
		Revisió independent de la seguretat de la informació.	2			Com ja hem anat comentat existeixen varis procediments, polítiques i normes, però existeixen deficiències en els tres punts
		Compliment de les polítiques i normes de seguretat.	2			
		Comprovació del compliment tècnic.	2			

Taula 4. Anàlisi de compliment inicial dels controls de la ISO 27002

Els valors de compliment inicial de la implementació dels controls de la norma ISO/IEC 27001 es basen en el fet que:

- Les taques que s'han realitzat des de el departament de Sistemes i Tecnologies de la informació referent als usos i a les bones pràctiques seran la base de la política de seguretat del SGSI a implantar.
- Tot i que hi ha processos definits en quant a riscos i a gestió de incidents, aquest no estan gestionats de manera eficient ni se n'ha automatitzat el flux.
- La gestió dels actiu és un aspecte al que es vol posar fil a l'agulla a l'organització, ja que fins al moment no s'ha sabut gestionar correctament, tot i els esforços fets fins el moment.
- El que si s'ha treballat de forma correcta son els controls del punt A.9 tot i que s'han de millorar els fluxos i optimitzar processos.
- Els controls definits en els punts A.11 A.12 i A.13 són els que fan referència a la seguretat en els seus diferents camps, físic, operacions i comunicacions. Tot i que es disposa de recursos i infraestructura per tenir una millor puntuació, considerem que no s'està traient el rendiment necessari i que els processos no estan del tot definits i no s'ha format el suficient als treballadors i voluntaris que en fan ús.
- S'està treballant en un pla de continuïtat de negoci i s'estan realitzant inversions per millorar-la, aquest pla encara no s'ha tancat i està pendent de validació i comunicació.

En aquest gràfic podem observar els resultats obtinguts en la valoració inicial del compliment dels controls de la norma ISO/IEC 27002.

La línia vermella ens indica l'estat actual del compliment de la norma.

L'objectiu que es busca és el de tenir tots els controls siguin gestionats i es puguin mesurar que seria la línia groga.

En verd trobem l'estat de compliment òptim de la norma

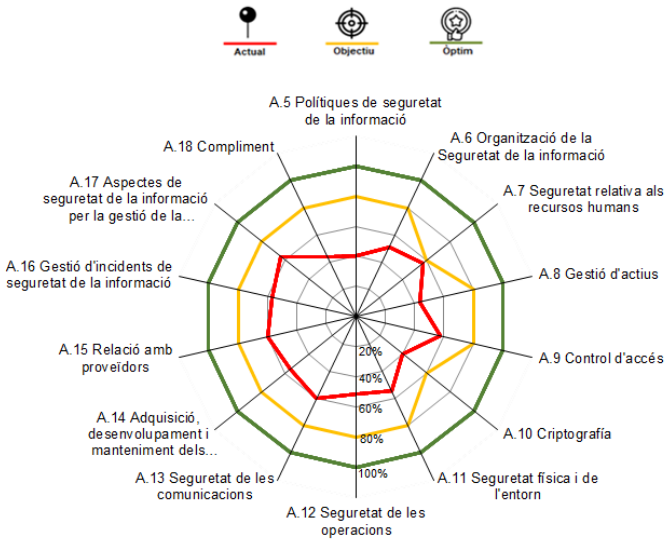

Figura 8. Anàlisi inicial GAP dels controls

A diferència dels requeriments de la norma, en els controls tenim que bona part ja estan definits o s'han reproduït, gràcies al treballs fets prèviament.

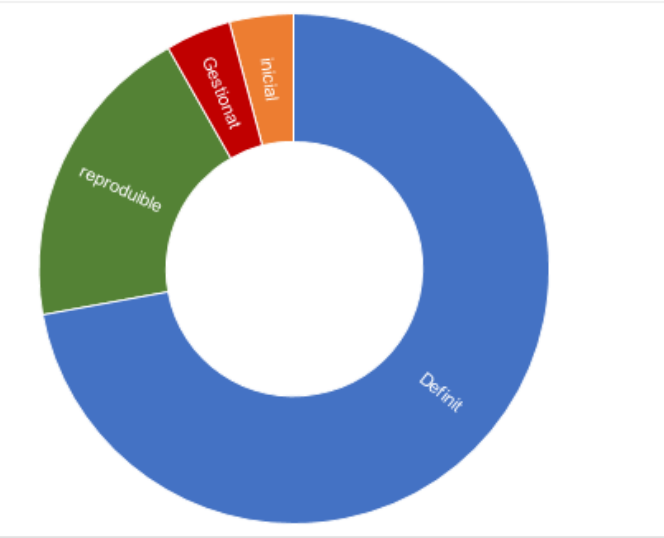

Figura 9. Nivells de Maduresa dels controls

3. Sistema de Gestió Documental

La norma ISO/IEC 27001 defineix quina és la documentació necessària per la correcte implementació i posterior certificació del sistema. Aquest sistema de Gestió documental és el conjunt de normes i definicions tècniques i pràctiques que s'han de portar a terme, i 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.

Tots els documents estan subjectes a un procés d'aprovació, així com a un procés de revisió i actualització periòdics per tal de valorar-ne l'efectivitat. El documents estaran vigents un cop aprovats per la direcció i estaran vigents fins a les noves revisions aprovades o fins que es produeixi un canvi substancial en a l'organització que afecti al SGSI amb el que els documents quedaran automàticament derogats a l'espera d'una revisió i actualització immediata per part del comitè de seguretat i la direcció.

3.1 Política de Seguretat

La política de seguretat de la informació és un document breu i d'alt nivell que detalla el principal objectiu del SGSI, defineix les mesures tècniques i organitzatives i descriu breument els rols i les responsabilitats en referència a la seguretat de la informació.

Aquesta política es troba detallada a l'Annex 1 Política de seguretat.

3.2 Procediment d'auditories internes

Tal i com s'indica a la Norma de la ISO/IEC 27001 [1] en el seu punt 9.2 Auditories internes, la organització a de dur a terme auditories internes en intervals planificats, per proporcionar informació sobre si l'SGSI compleix amb els requisits propis i els de la norma seleccionada implantada.

Aquest procediment es troba detallat a l'Annex 2 Procediment d'auditories internes.

3.3 Gestió d'indicadors

Per tal d'avaluar, monitoritzar i revisar els sistema i els controls implementats cal establir una sèrie d'indicadors que ens permetin realitzar aquesta tasca.

Aquest indicadors es troben definits a l'annex 3.

3.4 Procediment de revisió per direcció

Tal i com indica la norma ISO/IEC 27001 [1] en el seu punt 9.3, l'alta direcció ha de revisar el sistema de gestió de la seguretat de la informació en intervals planificats, per assegurar la seva conveniència, adequació i eficàcia continua.

La formació i funcionalitats d'aquest comitè es troben descrites a l'Annex 4.

3.5 Gestió de rols i responsabilitats

Tal i com indica la norma ISO/IEC 27001 [1] en el seu punt 5.3, l'alta direcció s'ha d'assegurar que les responsabilitats i autoritats pels rols pertinents a la seguretat de la informació s'assignen i comuniquen dins de l'organització.

A tal efecte també es crea un comitè de seguretat que es l'encarregat d'elaborar, coordinar i fer complir l'SGSI.

Aquests rols i responsabilitats es troben definits en l'Annex 5.

3.6 Metodologia d'anàlisi de riscos

És molt importat identificar els actius d'informació i establir el risc a què estan sotmesos per poder determinar així quin serà l'impacte per l'organització si es produeix una falta de disponibilitat, integritat o confidencialitat. La determinació del risc real a la que estan sotmesos els actius de l'organització permetrà a la direcció prendre les decisions sobre quin és el llindar de risc acceptable i prioritzar les accions en matèria de seguretat de la informació amb mesures proporcionades [6].

La metodologia de l'anàlisi de riscos la trobem desenvolupada a l'Annex 6.

3.7 Declaració d'aplicabilitat

La declaració d'aplicabilitat és un document que recull la relació de controls de la ISO/IEC 27002, especificant per cadascun d'ells, si és d'aplicació o no a la organització, juntament amb la seva justificació i si ja hi ha alguna mena de control implementat a l'actualitat [6].

La declaració d'aplicabilitat la trobem adjunta a l'Annex 7.

4. Anàlisi de Riscos

Tal i com s'ha descrit en els procediments de l'anàlisi de riscos que trobem a l'annex 6 seguirem la metodologia Magerit, perquè aquesta metodologia i no un altre, doncs perquè aquesta metodologia ens permet fer un anàlisi tant quantitatiu com qualitatiu, en l'anàlisi quantitatiu podem expressar ja amb el seu valor econòmic el risc. No obstant, aquí farem un anàlisi qualitatiu, amb els valors que es troben descrits a l'annex indicat. El pas de qualitatiu a quantitatiu no es complicat.

Per començar amb l'anàlisi revisem que estan involucrats en el sistema de informació a analitzar i que trobem a la Taula 1 de l'apartat 2 del treball.

Un cop revisats els elements que componen l'inventari valorem quina dependència existeix entre aquests actius, ja que aquesta relació té incidència directe en l'anàlisi que es fa de la valoració del risc.

		Actius d'equipament i aplicacions																	
		CPDs	Routers i Switchs	Firewalls	IDS/IPS	Servidors Producció	Servidors Backup	Servidors correu	Entorn de proves	Cabina de discs (emmagatzematge de xarxa)	Xarxa DMZ	Accés Xarxa Pública	Accés Xarxa Privada	Plataforma corporativa	Gestor Base de Dades	Office 365 corp	Control de portes	Càmeres Seguretat	Robot de cintes
Actius d'informació i serveis	Fitxers personals	x	x	x	x		x			x	x		x			x			x
	Bases de dades Aplicacions	x	x	x	x	x	x			x	x		x	x	x	x			x
	Copies de Seguretat	x	x	x	x		x			x			x		x				x
	Bases de dades Gestió interna	x	x	x	x	x	x			x			x	x	x	x			x
	Dades control accés	x	x	x	x	x				x			x		x		x		x
	Codis font desenvolupament	x	x	x	x				x	x			x						x
	Registres	x	x			x				x									x
	videovigilància	x																x	
	Certificats	x								x		x							x
	Directori Actiu	x				x	x				x		x						
	Web	x	x	x	x	x	x				x	x							x
	Serveis al usuari final	x	x	x	x	x	x				x	x	x	x	x	x			x
	VPN	x	x	x	x	x	x				x	x	x	x	x	x			
	Intranet	x	x	x	x	x	x				x	x	x	x	x	x			
	O365 (correu i fitxers)	x	x	x	x			x			x	x				x			
	Emmagatzematge de dades local	x	x							x									x

Taula 5. Dependència entre actius

El següent pas és el de valorar quina importància té per l'organització cada un dels actius, també cal valorar cadascun d'aquest actius en cadascuna de les dimensions de seguretat definides.
El actius es veuen afectats per amenaces, però quines amenaces i a quines dimensions afecten a cadascun del actius? Aquestes amenaces i les dimensions a les que afecten les trobem descrites al llibre 2 de magerit [5].

Origen	ID. A	Amenaça	Dimensions					Tipus d'actius									
			A	C	I	D	T	L	HW	SW	D	KY	COM	S	MED	AUX	P
Desastres naturals	N.1	Foc	NO	NO	NO	SI	NO	SI	SI	NO	NO	NO	NO	NO	SI	SI	NO
	N.2	Danys per aigua	NO	NO	NO	SI	NO	SI	SI	NO	NO	NO	NO	NO	SI	SI	NO
	N.9	Origen meteorològic	NO	NO	NO	SI	NO	SI	SI	NO	NO	NO	NO	NO	SI	SI	NO
Origen Industrial	I.5	Averia d'origen físic o lògic	NO	NO	NO	SI	NO	NO	SI	SI	NO	NO	NO	NO	SI	SI	NO
	I.6	Tall elèctric	NO	NO	NO	SI	NO	NO	SI	NO	NO	NO	NO	NO	SI	SI	NO
	I.7	Condicions inadequades Temperatura o humitat	NO	NO	NO	SI	NO	NO	SI	NO	NO	NO	NO	NO	SI	SI	NO
	I.8	Fallada servei comunicacions	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	I.9	Interrupció d'altres serveis	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
	I.10	Degradació dels suports d'emmagatzematge	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO	NO
Errors i fallades no intencionades	E.1	Errors d'usuaris	NO	SI	SI	SI	NO	NO	NO	SI	SI	SI	NO	SI	SI	NO	NO
	E.2	Erros d'administrador	NO	SI	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI	SI	NO	NO
	E.7	Deficiències amb la organització	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI
	E.8	Difusió de software maligne	NO	SI	SI	SI	SI	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO
	E.15	Alteració accidental de la informació	NO	NO	SI	NO	SI	NO	NO	SI	SI	SI	SI	SI	SI	NO	NO
	E.18	Destrucció de la informació	NO	NO	NO	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI	NO	NO
	E.19	Fuga de informació	NO	SI	NO	NO	NO	NO	NO	SI	SI	SI	SI	SI	SI	NO	SI
	E.20	Vulnerabilitat dels programes	NO	SI	SI	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO
	E.21	Errors manteniment o actualització de programes	NO	NO	SI	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO
	E.23	Errors manteniment o actualització d'equips	NO	NO	NO	SI	NO	NO	SI	NO	NO	NO	SI	SI	NO	NO	NO
	E.24	Caiguda de sistema per esgotament de recursos	NO	NO	NO	SI	NO	NO	SI	NO	NO	NO	SI	SI	NO	NO	NO
	E.25	Pèrdua d'equips	NO	SI	NO	SI	NO	NO	SI	NO	NO	NO	NO	NO	SI	SI	NO
	E.28	Indisponiblitat del personal	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI
Atacs Intencionats	A.4	Manipulació de la informació	SI	SI	SI	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO
	A.5	Suplantació d'identitat	SI	SI	SI	NO	NO	NO	NO	SI	SI	SI	SI	SI	NO	NO	NO
	A.6	Abús de privilegis d'accés	NO	SI	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI	NO	NO	NO
	A.7	Ús no previst	NO	SI	SI	SI	NO	SI	SI	SI	NO	NO	SI	SI	SI	SI	NO
	A.8	Difusió de software maligne	NO	SI	SI	SI	SI	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO
	A.11	Accés no autoritzat	NO	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO
	A.15	Modificació deliberada de la informació	NO	NO	SI	NO	NO	NO	NO	SI	SI	SI	SI	SI	SI	NO	NO
	A.18	Destrucció de la informació	NO	NO	NO	SI	SI	NO	NO	SI	SI	SI	NO	SI	SI	NO	NO
	A.19	Divulgació de informació	NO	SI	NO	NO	NO	NO	NO	SI	SI	SI	SI	SI	SI	NO	NO
	A.24	Denegació de servei	NO	NO	NO	SI	NO	NO	SI	SI	NO	NO	SI	SI	NO	NO	NO
	A.25	Robatori	NO	SI	NO	SI	NO	NO	SI	SI	NO	NO	NO	NO	SI	SI	NO
	A.28	Indisponiblitat del personal	NO	NO	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI
	A.29	Extorsió	NO	SI	SI	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI
	A.30	Enginyeria social	NO	SI	SI	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI

Taula 6. Llistat i classificació d'amenaces

Un cop definides les amenaces i els actius definim com afecten aquestes amenaces en cadascun dels actius. El resultat obtingut és l'impacte. A les següents taules veurem quin es l'impacte en cadascun dels actius, s'han agrupat les taules per tipus d'actius per poder-ne fer un millor seguiment.

Les taules que mesuren l'impacte son les que van de la Taula 7 a la 16.

Després de l'impacte toca valorar el Risc, el risc tal i com s'indica l'annex 6 es calcula amb la probabilitat que succeeixi una amenaça i amb l'impacte. El càlcul el podem trobar a les Taules de la 17 a la 26.

4.1 Valoració i Impacte dels actius

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
L.1	Edificis	A	N.1	Foc	0	8	4	8	0				100%					8,00	
			N.2	Danys per aigua	0	8	4	8	0				50%					4,00	
			N.9	Origen meteorològic	0	8	4	8	0				5%					0,40	
			A.7	Ús no previst	0	8	4	8	0		20%	20%	20%			1,60	0,80	1,60	
			A.11	Accés no autoritzat	0	8	4	8	0		75%	20%				6,00	0,80		
L.2	CPDs	MA	N.1	Foc	10	10	10	10	10				100%					10,00	
			N.2	Danys per aigua	10	10	10	10	10				100%					10,00	
			N.9	Origen meteorològic	10	10	10	10	10				5%					0,50	
			A.7	Ús no previst	10	10	10	10	10		100%	75%	75%			10,00	7,50	7,50	
			A.11	Accés no autoritzat	10	10	10	10	10		100%	20%				10,00	2,00		
L.3	Centre de Backup	MA	N.1	Foc	9	9	9	9	9				100%					9,00	
			N.2	Danys per aigua	9	9	9	9	9				50%					4,50	
			N.9	Origen meteorològic	9	9	9	9	9				5%					0,45	
			A.7	Ús no previst	9	9	9	9	9		20%	20%	20%			1,80	1,80	1,80	
			A.11	Accés no autoritzat	9	9	9	9	9		50%	20%				4,50	1,80		

Taula 7. Valoració i Impacte actius d'instal·lacions

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
HW.1	Routers i Switchs	MA	N.1	Foc	9	9	9	10	10				100%					10,00	
			N.2	Danys per aigua	9	9	9	10	10				100%					10,00	
			N.9	Origen meteorològic	9	9	9	10	10				100%					10,00	
			I.5	Averia d'origen físic o lògic	9	9	9	10	10				100%					10,00	
			I.6	Tall elèctric	9	9	9	10	10				100%					10,00	
			I.7	Condicions inadequades Temperatura o humitat	9	9	9	10	10				100%					10,00	
			E.2	Erros d'administrador	9	9	9	10	10		5%	5%	100%			0,45	0,45	10,00	
			E.23	Errors manteniment o actualització d'equips	9	9	9	10	10				100%					10,00	
			E.24	Caiguda de sistema per esgotament de recursos	9	9	9	10	10				100%					10,00	
			E.25	Pèrdua d'equips	9	9	9	10	10		20%		100%			1,80		10,00	

			A.6	Abús de privilegis d'accés	9	9	9	10	10		20%	20%	20%			1,80	1,80	2,00	
			A.7	Ús no previst	9	9	9	10	10		100%	20%	100%			9,00	1,80	10,00	
			A.11	Accés no autoritzat	9	9	9	10	10		100%	20%				9,00	1,80		
			A.24	Denegació de servei	9	9	9	10	10				100%					10,00	
			A.25	Robatori	9	9	9	10	10		20%		100%			1,80		10,00	
HW.2	Firewalls	MA	N.1	Foc	10	9	9	10	10				100%					10,00	
			N.2	Danys per aigua	10	9	9	10	10				100%					10,00	
			N.9	Origen meteorològic	10	9	9	10	10				100%					10,00	
			I.5	Averia d'origen físic o lògic	10	9	9	10	10				100%					10,00	
			I.6	Tall elèctric	10	9	9	10	10				100%					10,00	
			I.7	Condicions inadequades Temperatura o humitat	10	9	9	10	10				100%					10,00	
			E.2	Erros d'administrador	10	9	9	10	10		5%	5%	100%			0,45	0,45	10,00	
			E.23	Errors manteniment o actualització d'equips	10	9	9	10	10				100%					10,00	
			E.24	Caiguda de sistema per esgotament de recursos	10	9	9	10	10				100%					10,00	
			E.25	Pèrdua d'equips	10	9	9	10	10		20%		100%			1,80		10,00	
			A.6	Abús de privilegis d'accés	10	9	9	10	10		20%	20%	20%			1,80	1,80	2,00	
			A.7	Ús no previst	10	9	9	10	10		100%	20%	100%			9,00	1,80	10,00	
			A.11	Accés no autoritzat	10	9	9	10	10		100%	20%				9,00	1,80		
			A.24	Denegació de servei	10	9	9	10	10				100%					10,00	
			A.25	Robatori	10	9	9	10	10		20%		100%			1,80		10,00	
HW.3	IDS/IPS	MA	N.1	Foc	10	10	9	10	10				100%					10,00	
			N.2	Danys per aigua	10	10	9	10	10				100%					10,00	
			N.9	Origen meteorològic	10	10	9	10	10				100%					10,00	
			I.5	Averia d'origen físic o lògic	10	10	9	10	10				100%					10,00	
			I.6	Tall elèctric	10	10	9	10	10				100%					10,00	
			I.7	Condicions inadequades Temperatura o humitat	10	10	9	10	10				100%					10,00	
			E.2	Erros d'administrador	10	10	9	10	10		5%	5%	100%			0,50	0,45	10,00	
			E.23	Errors manteniment o actualització d'equips	10	10	9	10	10				100%					10,00	
			E.24	Caiguda de sistema per esgotament de recursos	10	10	9	10	10				100%					10,00	
			E.25	Pèrdua d'equips	10	10	9	10	10		20%		100%			2,00		10,00	
			A.6	Abús de privilegis d'accés	10	10	9	10	10		20%	20%	20%			2,00	1,80	2,00	
			A.7	Ús no previst	10	10	9	10	10		100%	20%	100%			10,00	1,80	10,00	
			A.11	Accés no autoritzat	10	10	9	10	10		100%	20%				10,00	1,80		
			A.24	Denegació de servei	10	10	9	10	10				100%					10,00	

			A.25	Robatori	10	10	9	10	10		20%		100%			2,00		10,00	
HW.4	AP's	B	N.1	Foc	3	3	3	3	3				100%					3,00	
			N.2	Danys per aigua	3	3	3	3	3				100%					3,00	
			N.9	Origen meteorològic	3	3	3	3	3				100%					3,00	
			I.5	Averia d'origen físic o lògic	3	3	3	3	3				100%					3,00	
			I.6	Tall elèctric	3	3	3	3	3				100%					3,00	
			I.7	Condicions inadequades Temperatura o humitat	3	3	3	3	3				100%					3,00	
			E.2	Erros d'administrador	3	3	3	3	3		5%	5%	100%			0,15	0,15	3,00	
			E.23	Errors manteniment o actualització d'equips	3	3	3	3	3				100%					3,00	
			E.24	Caiguda de sistema per esgotament de recursos	3	3	3	3	3				100%					3,00	
			E.25	Pèrdua d'equips	3	3	3	3	3		20%		100%			0,60		3,00	
			A.6	Abús de privilegis d'accés	3	3	3	3	3		20%	20%	20%			0,60	0,60	0,60	
			A.7	Ús no previst	3	3	3	3	3		100%	20%	100%			3,00	0,60	3,00	
			A.11	Accés no autoritzat	3	3	3	3	3		100%	20%				3,00	0,60		
			A.24	Denegació de servei	3	3	3	3	3				100%					3,00	
			A.25	Robatori	3	3	3	3	3		20%		100%			0,60		3,00	
HW.5	Servidors Producció	MA	N.1	Foc	10	8	8	9	9				100%					9,00	
			N.2	Danys per aigua	10	8	8	9	9				100%					9,00	
			N.9	Origen meteorològic	10	8	8	9	9				100%					9,00	
			I.5	Averia d'origen físic o lògic	10	8	8	9	9				100%					9,00	
			I.6	Tall elèctric	10	8	8	9	9				100%					9,00	
			I.7	Condicions inadequades Temperatura o humitat	10	8	8	9	9				100%					9,00	
			E.2	Erros d'administrador	10	8	8	9	9		5%	5%	100%			0,40	0,40	9,00	
			E.23	Errors manteniment o actualització d'equips	10	8	8	9	9				100%					9,00	
			E.24	Caiguda de sistema per esgotament de recursos	10	8	8	9	9				100%					9,00	
			E.25	Pèrdua d'equips	10	8	8	9	9		20%		100%			1,60		9,00	
			A.6	Abús de privilegis d'accés	10	8	8	9	9		20%	20%	100%			1,60	1,60	9,00	
			A.7	Ús no previst	10	8	8	9	9		100%	20%	100%			8,00	1,60	9,00	
			A.11	Accés no autoritzat	10	8	8	9	9		100%	20%				8,00	1,60		
			A.24	Denegació de servei	10	8	8	9	9				100%					9,00	
			A.25	Robatori	10	8	8	9	9		20%		100%			1,60		9,00	
HW.6	Servidors Backup	MA	N.1	Foc	8	8	8	10	8				100%					10,00	
			N.2	Danys per aigua	8	8	8	10	8				100%					10,00	
			N.9	Origen meteorològic	8	8	8	10	8				100%					10,00	

			I.5	Averia d'origen físic o lògic	8	8	8	10	8				100%					10,00	
			I.6	Tall elèctric	8	8	8	10	8				100%					10,00	
			I.7	Condicions inadequades Temperatura o humitat	8	8	8	10	8				100%					10,00	
			E.2	Erros d'administrador	8	8	8	10	8		5%	5%	100%			0,40	0,40	10,00	
			E.23	Errors manteniment o actualització d'equips	8	8	8	10	8				100%					10,00	
			E.24	Caiguda de sistema per esgotament de recursos	8	8	8	10	8				100%					10,00	
			E.25	Pèrdua d'equips	8	8	8	10	8		20%		100%			1,60		10,00	
			A.6	Abús de privilegis d'accés	8	8	8	10	8		20%	20%	100%			1,60	1,60	10,00	
			A.7	Ús no previst	8	8	8	10	8		100%	20%	100%			8,00	1,60	10,00	
			A.11	Accés no autoritzat	8	8	8	10	8		100%	20%				8,00	1,60		
			A.24	Denegació de servei	8	8	8	10	8				100%					10,00	
			A.25	Robatori	8	8	8	10	8		20%		100%			1,60		10,00	
HW.7	Servidors correu	B	N.1	Foc	3	3	3	3	3				100%					3,00	
			N.2	Danys per aigua	3	3	3	3	3				100%					3,00	
			N.9	Origen meteorològic	3	3	3	3	3				100%					3,00	
			I.5	Averia d'origen físic o lògic	3	3	3	3	3				100%					3,00	
			I.6	Tall elèctric	3	3	3	3	3				100%					3,00	
			I.7	Condicions inadequades Temperatura o humitat	3	3	3	3	3				100%					3,00	
			E.2	Erros d'administrador	3	3	3	3	3		5%	5%	100%			0,15	0,15	3,00	
			E.23	Errors manteniment o actualització d'equips	3	3	3	3	3				100%					3,00	
			E.24	Caiguda de sistema per esgotament de recursos	3	3	3	3	3				100%					3,00	
			E.25	Pèrdua d'equips	3	3	3	3	3		20%		100%			0,60		3,00	
			A.6	Abús de privilegis d'accés	3	3	3	3	3		20%	20%	100%			0,60	0,60	3,00	
			A.7	Ús no previst	3	3	3	3	3		100%	20%	100%			3,00	0,60	3,00	
			A.11	Accés no autoritzat	3	3	3	3	3		100%	20%				3,00	0,60		
			A.24	Denegació de servei	3	3	3	3	3				100%					3,00	
			A.25	Robatori	3	3	3	3	3		20%		100%			0,60		3,00	
HW.8	Entorn de proves	B	N.1	Foc	3	3	3	3	3				100%					3,00	
			N.2	Danys per aigua	3	3	3	3	3				100%					3,00	
			N.9	Origen meteorològic	3	3	3	3	3				100%					3,00	
			I.5	Averia d'origen físic o lògic	3	3	3	3	3				100%					3,00	
			I.6	Tall elèctric	3	3	3	3	3				100%					3,00	
			I.7	Condicions inadequades Temperatura o humitat	3	3	3	3	3				100%					3,00	
			E.2	Erros d'administrador	3	3	3	3	3		5%	5%	100%			0,15	0,15	3,00	

			E.23	Errors manteniment o actualització d'equips	3	3	3	3	3				100%					3,00	
			E.24	Caiguda de sistema per esgotament de recursos	3	3	3	3	3				100%					3,00	
			E.25	Pèrdua d'equips	3	3	3	3	3		20%		100%			0,60		3,00	
			A.6	Abús de privilegis d'accés	3	3	3	3	3		20%	20%	100%			0,60	0,60	3,00	
			A.7	Ús no previst	3	3	3	3	3		100%	20%	100%			3,00	0,60	3,00	
			A.11	Accés no autoritzat	3	3	3	3	3		100%	20%				3,00	0,60		
			A.24	Denegació de servei	3	3	3	3	3				100%					3,00	
			A.25	Robatori	3	3	3	3	3		20%		100%			0,60		3,00	
HW.9	Telèfons IP	B	N.1	Foc	2	2	2	2	2				100%					2,00	
			N.2	Danys per aigua	2	2	2	2	2				100%					2,00	
			N.9	Origen meteorològic	2	2	2	2	2				100%					2,00	
			I.5	Averia d'origen físic o lògic	2	2	2	2	2				100%					2,00	
			I.6	Tall elèctric	2	2	2	2	2				100%					2,00	
			I.7	Condicions inadequades Temperatura o humitat	2	2	2	2	2				100%					2,00	
			E.2	Erros d'administrador	2	2	2	2	2		5%	5%	100%			0,10	0,10	2,00	
			E.23	Errors manteniment o actualització d'equips	2	2	2	2	2				100%					2,00	
			E.24	Caiguda de sistema per esgotament de recursos	2	2	2	2	2				100%					2,00	
			E.25	Pèrdua d'equips	2	2	2	2	2		20%		100%			0,40		2,00	
			A.6	Abús de privilegis d'accés	2	2	2	2	2		20%	20%	20%			0,40	0,40	0,40	
			A.7	Ús no previst	2	2	2	2	2		100%	20%	100%			2,00	0,40	2,00	
			A.11	Accés no autoritzat	2	2	2	2	2		100%	20%				2,00	0,40		
			A.24	Denegació de servei	2	2	2	2	2				100%					2,00	
			A.25	Robatori	2	2	2	2	2		20%		100%			0,40		2,00	
HW.10	Telèfons mòbils	M	N.1	Foc	4	8	4	4	5				100%					4,00	
			N.2	Danys per aigua	4	8	4	4	5				100%					4,00	
			N.9	Origen meteorològic	4	8	4	4	5				100%					4,00	
			I.5	Averia d'origen físic o lògic	4	8	4	4	5				100%					4,00	
			I.6	Tall elèctric	4	8	4	4	5				100%					4,00	
			I.7	Condicions inadequades Temperatura o humitat	4	8	4	4	5				100%					4,00	
			E.2	Erros d'administrador	4	8	4	4	5		5%	5%	100%			0,40	0,20	4,00	
			E.23	Errors manteniment o actualització d'equips	4	8	4	4	5				100%					4,00	
			E.24	Caiguda de sistema per esgotament de recursos	4	8	4	4	5				100%					4,00	
			E.25	Pèrdua d'equips	4	8	4	4	5		20%		100%			1,60		4,00	
			A.6	Abús de privilegis d'accés	4	8	4	4	5		20%	20%	20%			1,60	0,80	0,80	

			A.7	Ús no previst	4	8	4	4	5		100%	20%	100%			8,00	0,80	4,00	
			A.11	Accés no autoritzat	4	8	4	4	5		100%	20%				8,00	0,80		
			A.24	Denegació de servei	4	8	4	4	5				100%					4,00	
			A.25	Robatori	4	8	4	4	5		20%		100%			1,60		4,00	
HW.11	Portàtils	M	N.1	Foc	4	8	4	4	5				100%					4,00	
			N.2	Danys per aigua	4	8	4	4	5				100%					4,00	
			N.9	Origen meteorològic	4	8	4	4	5				100%					4,00	
			I.5	Averia d'origen físic o lògic	4	8	4	4	5				100%					4,00	
			I.6	Tall elèctric	4	8	4	4	5				100%					4,00	
			I.7	Condicions inadequades Temperatura o humitat	4	8	4	4	5				100%					4,00	
			E.2	Erros d'administrador	4	8	4	4	5		5%	5%	100%			0,40	0,20	4,00	
			E.23	Errors manteniment o actualització d'equips	4	8	4	4	5				100%					4,00	
			E.24	Caiguda de sistema per esgotament de recursos	4	8	4	4	5				100%					4,00	
			E.25	Pèrdua d'equips	4	8	4	4	5		20%		100%			1,60		4,00	
			A.6	Abús de privilegis d'accés	4	8	4	4	5		20%	20%	20%			1,60	0,80	0,80	
			A.7	Ús no previst	4	8	4	4	5		20%	20%	100%			1,60	0,80	4,00	
			A.11	Accés no autoritzat	4	8	4	4	5		20%	20%				1,60	0,80		
			A.24	Denegació de servei	4	8	4	4	5				100%					4,00	
			A.25	Robatori	4	8	4	4	5		20%		100%			1,60		4,00	
HW.12	PC's usuari i ús genèric	M	N.1	Foc	4	8	4	5	3				100%					5,00	
			N.2	Danys per aigua	4	8	4	5	3				100%					5,00	
			N.9	Origen meteorològic	4	8	4	5	3				100%					5,00	
			I.5	Averia d'origen físic o lògic	4	8	4	5	3				100%					5,00	
			I.6	Tall elèctric	4	8	4	5	3				100%					5,00	
			I.7	Condicions inadequades Temperatura o humitat	4	8	4	5	3				100%					5,00	
			E.2	Erros d'administrador	4	8	4	5	3		5%	5%	100%			0,40	0,20	5,00	
			E.23	Errors manteniment o actualització d'equips	4	8	4	5	3				100%					5,00	
			E.24	Caiguda de sistema per esgotament de recursos	4	8	4	5	3				100%					5,00	
			E.25	Pèrdua d'equips	4	8	4	5	3		20%		100%			1,60		5,00	
			A.6	Abús de privilegis d'accés	4	8	4	5	3		20%	20%	20%			1,60	0,80	1,00	
			A.7	Ús no previst	4	8	4	5	3		20%	20%	100%			1,60	0,80	5,00	
			A.11	Accés no autoritzat	4	8	4	5	3		20%	20%				1,60	0,80		
			A.24	Denegació de servei	4	8	4	5	3				100%					5,00	
			A.25	Robatori	4	8	4	5	3		20%		100%			1,60		5,00	

HW.13	PC's accés públic	MB	N.1	Foc	0	0	0	2	0				100%					2,00	
			N.2	Danys per aigua	0	0	0	2	0				100%					2,00	
			N.9	Origen meteorològic	0	0	0	2	0				100%					2,00	
			I.5	Averia d'origen físic o lògic	0	0	0	2	0				100%					2,00	
			I.6	Tall elèctric	0	0	0	2	0				100%					2,00	
			I.7	Condicions inadequades Temperatura o humitat	0	0	0	2	0				100%					2,00	
			E.2	Erros d'administrador	0	0	0	2	0		5%	5%	100%			0,00	0,00	2,00	
			E.23	Errors manteniment o actualització d'equips	0	0	0	2	0				100%					2,00	
			E.24	Caiguda de sistema per esgotament de recursos	0	0	0	2	0				100%					2,00	
			E.25	Pèrdua d'equips	0	0	0	2	0		20%		100%			0,00		2,00	
			A.6	Abús de privilegis d'accés	0	0	0	2	0		20%	20%	20%			0,00	0,00	0,40	
			A.7	Ús no previst	0	0	0	2	0		20%	20%	100%			0,00	0,00	2,00	
			A.11	Accés no autoritzat	0	0	0	2	0		20%	20%				0,00	0,00		
			A.24	Denegació de servei	0	0	0	2	0				100%					2,00	
			A.25	Robatori	0	0	0	2	0		20%		100%			0,00		2,00	
HW.14	Impressores	M	N.1	Foc	0	5	4	4	0				100%					4,00	
			N.2	Danys per aigua	0	5	4	4	0				100%					4,00	
			N.9	Origen meteorològic	0	5	4	4	0				100%					4,00	
			I.5	Averia d'origen físic o lògic	0	5	4	4	0				100%					4,00	
			I.6	Tall elèctric	0	5	4	4	0				100%					4,00	
			I.7	Condicions inadequades Temperatura o humitat	0	5	4	4	0				100%					4,00	
			E.2	Erros d'administrador	0	5	4	4	0		5%	5%	100%			0,25	0,20	4,00	
			E.23	Errors manteniment o actualització d'equips	0	5	4	4	0				100%					4,00	
			E.24	Caiguda de sistema per esgotament de recursos	0	5	4	4	0				100%					4,00	
			E.25	Pèrdua d'equips	0	5	4	4	0		5%		100%			0,25		4,00	
			A.6	Abús de privilegis d'accés	0	5	4	4	0		5%	5%	20%			0,25	0,20	0,80	
			A.7	Ús no previst	0	5	4	4	0		5%	5%	50%			0,25	0,20	2,00	
			A.11	Accés no autoritzat	0	5	4	4	0		5%	5%				0,25	0,20		
			A.24	Denegació de servei	0	5	4	4	0				100%					4,00	
			A.25	Robatori	0	5	4	4	0		5%		100%			0,25		4,00	
HW.15	Escàners	M	N.1	Foc	0	3	4	5	0				100%					5,00	
			N.2	Danys per aigua	0	3	4	5	0				100%					5,00	
			N.9	Origen meteorològic	0	3	4	5	0				100%					5,00	
			I.5	Averia d'origen físic o lògic	0	3	4	5	0				100%					5,00	

			I.6	Tall elèctric	0	3	4	5	0				100%					5,00	
			I.7	Condicions inadequades Temperatura o humitat	0	3	4	5	0				100%					5,00	
			E.2	Erros d'administrador	0	3	4	5	0		5%	20%	100%			0,15	0,80	5,00	
			E.23	Errors manteniment o actualització d'equips	0	3	4	5	0				100%					5,00	
			E.24	Caiguda de sistema per esgotament de recursos	0	3	4	5	0				100%					5,00	
			E.25	Pèrdua d'equips	0	3	4	5	0		100%		100%			3,00		5,00	
			A.6	Abús de privilegis d'accés	0	3	4	5	0		50%	5%	20%			1,50	0,20	1,00	
			A.7	Ús no previst	0	3	4	5	0		100%	20%	50%			3,00	0,80	2,50	
			A.11	Accés no autoritzat	0	3	4	5	0		100%	20%				3,00	0,80		
			A.24	Denegació de servei	0	3	4	5	0				100%					5,00	
			A.25	Robatori	0	3	4	5	0		100%		100%			3,00		5,00	

Taula 8. Valoració i Impacte actius de Hardware

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
SW.1	Plataforma corporativa	MA	I.5	Averia d'origen físic o lògic	8	10	9	9	10				100%					9,00	
			E.1	Errors d'usuaris	8	10	9	9	10		5%	5%	5%			0,50	0,45	0,45	
			E.2	Erros d'administrador	8	10	9	9	10		50%	50%	50%			5,00	4,50	4,50	
			E.8	Difusió de software maligne	8	10	9	9	10		100%	100%	100%	50%		10,00	9,00	9,00	5,00
			E.15	Alteració accidental de la informació	8	10	9	9	10			20%		5%			1,80		0,50
			E.18	Destrucció de la informació	8	10	9	9	10				100%	75%				9,00	7,50
			E.19	Fuga de informació	8	10	9	9	10		100%					10,00			
			E.20	Vulnerabilitat dels programes	8	10	9	9	10		20%	50%	5%			2,00	4,50	0,45	
			E.21	Errors manteniment o actualització de programes	8	10	9	9	10			50%	50%				4,50	4,50	
			A.5	Suplantació d'identitat	8	10	9	9	10	100%	100%	5%			8,00	10,00	0,45		
			A.6	Abús de privilegis d'accés	8	10	9	9	10		20%	5%	5%			2,00	0,45	0,45	
			A.7	Ús no previst	8	10	9	9	10		5%	5%	5%			0,50	0,45	0,45	
			A.8	Difusió de software maligne	8	10	9	9	10		100%	5%	5%	50%		10,00	0,45	0,45	5,00
			A.11	Accés no autoritzat	8	10	9	9	10		100%	20%				10,00	1,80		
			A.15	Modificació deliberada de la informació	8	10	9	9	10			100%					9,00		
			A.18	Destrucció de la informació	8	10	9	9	10				100%	75%				9,00	7,50
			A.19	Divulgació de informació	8	10	9	9	10		100%					10,00			
SW.2	Gestor Base de Dades	MA	I.5	Averia d'origen físic o lògic	8	10	9	9	10				100%					9,00	
			E.1	Errors d'usuaris	8	10	9	9	10		5%	5%	5%			0,50	0,45	0,45	

			E.2	Erros d'administrador	8	10	9	9	10		50%	50%	50%			5,00	4,50	4,50	
			E.8	Difusió de software maligne	8	10	9	9	10		100%	100%	100%	50%		10,00	9,00	9,00	5,00
			E.15	Alteració accidental de la informació	8	10	9	9	10			20%		5%			1,80		0,50
			E.18	Destrucció de la informació	8	10	9	9	10				100%	75%				9,00	7,50
			E.19	Fuga de informació	8	10	9	9	10		100%					10,00			
			E.20	Vulnerabilitat dels programes	8	10	9	9	10		20%	50%	5%			2,00	4,50	0,45	
			E.21	Errors manteniment o actualització de programes	8	10	9	9	10			50%	50%				4,50	4,50	
			A.5	Suplantació d'identitat	8	10	9	9	10	100%	100%	5%			8,00	10,00	0,45		
			A.6	Abús de privilegis d'accés	8	10	9	9	10		20%	5%	5%			2,00	0,45	0,45	
			A.7	Ús no previst	8	10	9	9	10		5%	5%	5%			0,50	0,45	0,45	
			A.8	Difusió de software maligne	8	10	9	9	10		100%	5%	5%	50%		10,00	0,45	0,45	5,00
			A.11	Accés no autoritzat	8	10	9	9	10		100%	20%				10,00	1,80		
			A.15	Modificació deliberada de la informació	8	10	9	9	10			100%					9,00		
			A.18	Destrucció de la informació	8	10	9	9	10				100%	75%				9,00	7,50
			A.19	Divulgació de informació	8	10	9	9	10		100%					10,00			
SW.3	Office 365 corp	B	I.5	Averia d'origen físic o lògic	3	3	3	3	3				100%					3,00	
			E.1	Errors d'usuaris	3	3	3	3	3		5%	5%	5%			0,15	0,15	0,15	
			E.2	Erros d'administrador	3	3	3	3	3		50%	50%	50%			1,50	1,50	1,50	
			E.8	Difusió de software maligne	3	3	3	3	3		100%	100%	100%	50%		3,00	3,00	3,00	1,50
			E.15	Alteració accidental de la informació	3	3	3	3	3			20%		5%			0,60		0,15
			E.18	Destrucció de la informació	3	3	3	3	3				100%	75%				3,00	2,25
			E.19	Fuga de informació	3	3	3	3	3		100%					3,00			
			E.20	Vulnerabilitat dels programes	3	3	3	3	3		20%	50%	5%			0,60	1,50	0,15	
			E.21	Errors manteniment o actualització de programes	3	3	3	3	3			50%	50%				1,50	1,50	
			A.5	Suplantació d'identitat	3	3	3	3	3	100%	100%	5%			3,00	3,00	0,15		
			A.6	Abús de privilegis d'accés	3	3	3	3	3		20%	5%	5%			0,60	0,15	0,15	
			A.7	Ús no previst	3	3	3	3	3		5%	5%	5%			0,15	0,15	0,15	
			A.8	Difusió de software maligne	3	3	3	3	3		100%	5%	5%	50%		3,00	0,15	0,15	1,50
			A.11	Accés no autoritzat	3	3	3	3	3		100%	20%				3,00	0,60		
			A.15	Modificació deliberada de la informació	3	3	3	3	3			100%					3,00		
			A.18	Destrucció de la informació	3	3	3	3	3				100%	75%				3,00	2,25
			A.19	Divulgació de informació	3	3	3	3	3		100%					3,00			
SW.4	Antivirus	A	I.5	Averia d'origen físic o lògic	6	6	10	10	10				100%					10,00	
			E.1	Errors d'usuaris	6	6	10	10	10		5%	5%	5%			0,30	0,50	0,50	

			E.2	Erros d'administrador	6	6	10	10	10		50%	50%	50%			3,00	5,00	5,00	
			E.8	Difusió de software maligne	6	6	10	10	10		100%	100%	100%	50%		6,00	10,00	10,00	5,00
			E.15	Alteració accidental de la informació	6	6	10	10	10			20%		5%			2,00		0,50
			E.18	Destrucció de la informació	6	6	10	10	10				100%	75%				10,00	7,50
			E.19	Fuga de informació	6	6	10	10	10		100%					6,00			
			E.20	Vulnerabilitat dels programes	6	6	10	10	10		20%	50%	5%			1,20	5,00	0,50	
			E.21	Errors manteniment o actualització de programes	6	6	10	10	10			50%	50%				5,00	5,00	
			A.5	Suplantació d'identitat	6	6	10	10	10	100%	100%	5%			6,00	6,00	0,50		
			A.6	Abús de privilegis d'accés	6	6	10	10	10		20%	5%	5%			1,20	0,50	0,50	
			A.7	Ús no previst	6	6	10	10	10		5%	5%	5%			0,30	0,50	0,50	
			A.8	Difusió de software maligne	6	6	10	10	10		100%	5%	5%	50%		6,00	0,50	0,50	5,00
			A.11	Accés no autoritzat	6	6	10	10	10		100%	20%				6,00	2,00		
			A.15	Modificació deliberada de la informació	6	6	10	10	10			100%					10,00		
			A.18	Destrucció de la informació	6	6	10	10	10				100%	75%				10,00	7,50
			A.19	Divulgació de informació	6	6	10	10	10		100%					6,00			
SW.5	Sistemes operatius	MB	I.5	Averia d'origen físic o lògic	1	1	1	1	1				100%					1,00	
			E.1	Errors d'usuaris	1	1	1	1	1		5%	5%	5%			0,05	0,05	0,05	
			E.2	Erros d'administrador	1	1	1	1	1		50%	50%	50%			0,50	0,50	0,50	
			E.8	Difusió de software maligne	1	1	1	1	1		100%	100%	100%	50%		1,00	1,00	1,00	0,50
			E.15	Alteració accidental de la informació	1	1	1	1	1			20%		5%			0,20		0,05
			E.18	Destrucció de la informació	1	1	1	1	1				100%	75%				1,00	0,75
			E.19	Fuga de informació	1	1	1	1	1		100%					1,00			
			E.20	Vulnerabilitat dels programes	1	1	1	1	1		20%	50%	5%			0,20	0,50	0,05	
			E.21	Errors manteniment o actualització de programes	1	1	1	1	1			50%	50%				0,50	0,50	
			A.5	Suplantació d'identitat	1	1	1	1	1	100%	100%	5%			1,00	1,00	0,05		
			A.6	Abús de privilegis d'accés	1	1	1	1	1		20%	5%	5%			0,20	0,05	0,05	
			A.7	Ús no previst	1	1	1	1	1		5%	5%	5%			0,05	0,05	0,05	
			A.8	Difusió de software maligne	1	1	1	1	1		100%	5%	5%	50%		1,00	0,05	0,05	0,50
			A.11	Accés no autoritzat	1	1	1	1	1		100%	20%				1,00	0,20		
			A.15	Modificació deliberada de la informació	1	1	1	1	1			100%					1,00		
			A.18	Destrucció de la informació	1	1	1	1	1				100%	75%				1,00	0,75
			A.19	Divulgació de informació	1	1	1	1	1		100%					1,00			

Taula 9. Valoració i Impacte actius de Software

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
D.1	Fitxers personals	MB	E.1	Errors d'usuaris	5	9	8	6	6		100%	50%	50%			9,00	4,00	3,00	
			E.2	Erros d'administrador	5	9	8	6	6		100%	100%	100%			9,00	8,00	6,00	
			E.15	Alteració accidental de la informació	5	9	8	6	6			20%		20%			1,60		1,20
			E.18	Destrucció de la informació	5	9	8	6	6				100%	20%				6,00	1,20
			E.19	Fuga de informació	5	9	8	6	6		100%					9,00			
			A.4	Manipulació de la informació	5	9	8	6	6	100%	100%	100%		20%	5,00	9,00	8,00		1,20
			A.5	Suplantació d'identitat	5	9	8	6	6	100%	100%	20%			5,00	9,00	1,60		
			A.6	Abús de privilegis d'accés	5	9	8	6	6		20%	20%	20%			1,80	1,60	1,20	
			A.11	Accés no autoritzat	5	9	8	6	6		100%	20%				9,00	1,60		
			A.15	Modificació deliberada de la informació	5	9	8	6	6			100%					8,00		
			A.18	Destrucció de la informació	5	9	8	6	6				100%	20%				6,00	1,20
			A.19	Divulgació de informació	5	9	8	6	6		100%					9,00			
D.2	Bases de dades Aplicacions	A	E.1	Errors d'usuaris	8	10	10	8	9		100%	50%	50%			10,00	5,00	4,00	
			E.2	Erros d'administrador	8	10	10	8	9		100%	100%	100%			10,00	10,00	8,00	
			E.15	Alteració accidental de la informació	8	10	10	8	9			20%		20%			2,00		1,80
			E.18	Destrucció de la informació	8	10	10	8	9				100%	20%				8,00	1,80
			E.19	Fuga de informació	8	10	10	8	9		100%					10,00			
			A.4	Manipulació de la informació	8	10	10	8	9	100%	100%	100%		20%	8,00	10,00	10,00		1,80
			A.5	Suplantació d'identitat	8	10	10	8	9	100%	100%	20%			8,00	10,00	2,00		
			A.6	Abús de privilegis d'accés	8	10	10	8	9		20%	20%	20%			2,00	2,00	1,60	
			A.11	Accés no autoritzat	8	10	10	8	9		100%	20%				10,00	2,00		
			A.15	Modificació deliberada de la informació	8	10	10	8	9			100%					10,00		
			A.18	Destrucció de la informació	8	10	10	8	9				100%	20%				8,00	1,80
			A.19	Divulgació de informació	8	10	10	8	9		100%					10,00			
D.3	Copies de Seguretat	A	E.1	Errors d'usuaris	8	8	10	6	4		50%	50%	100%			4,00	5,00	6,00	
			E.2	Erros d'administrador	8	8	10	6	4		100%	100%	100%			8,00	10,00	6,00	
			E.15	Alteració accidental de la informació	8	8	10	6	4			100%		20%			10,00		0,80
			E.18	Destrucció de la informació	8	8	10	6	4				100%	20%				6,00	0,80
			E.19	Fuga de informació	8	8	10	6	4		100%					8,00			
			A.4	Manipulació de la informació	8	8	10	6	4	50%	75%	100%		20%	4,00	6,00	10,00		0,80
			A.5	Suplantació d'identitat	8	8	10	6	4	50%	100%	20%			4,00	8,00	2,00		

			A.6	Abús de privilegis d'accés	8	8	10	6	4		20%	20%	20%			1,60	2,00	1,20	
			A.11	Accés no autoritzat	8	8	10	6	4		100%	5%				8,00	0,50		
			A.15	Modificació deliberada de la informació	8	8	10	6	4			100%					10,00		
			A.18	Destrucció de la informació	8	8	10	6	4				100%	20%				6,00	0,80
			A.19	Divulgació de informació	8	8	10	6	4		100%					8,00			
D.4	Bases de dades Gestió interna	M	E.1	Errors d'usuaris	6	6	6	3	6		100%	50%	50%			6,00	3,00	1,50	
			E.2	Erros d'administrador	6	6	6	3	6		100%	100%	100%			6,00	6,00	3,00	
			E.15	Alteració accidental de la informació	6	6	6	3	6			20%		20%			1,20		1,20
			E.18	Destrucció de la informació	6	6	6	3	6				100%	20%				3,00	1,20
			E.19	Fuga de informació	6	6	6	3	6		100%					6,00			
			A.4	Manipulació de la informació	6	6	6	3	6	100%	100%	100%		20%	6,00	6,00	6,00		1,20
			A.5	Suplantació d'identitat	6	6	6	3	6	100%	100%	20%			6,00	6,00	1,20		
			A.6	Abús de privilegis d'accés	6	6	6	3	6		20%	20%	20%			1,20	1,20	0,60	
			A.11	Accés no autoritzat	6	6	6	3	6		100%	20%				6,00	1,20		
			A.15	Modificació deliberada de la informació	6	6	6	3	6			100%					6,00		
			A.18	Destrucció de la informació	6	6	6	3	6				100%	20%				3,00	1,20
			A.19	Divulgació de informació	6	6	6	3	6		100%					6,00			
D.5	Dades control accés	B	E.1	Errors d'usuaris	3	6	6	3	2		50%	100%	100%			3,00	6,00	3,00	
			E.2	Erros d'administrador	3	6	6	3	2		100%	100%	100%			6,00	6,00	3,00	
			E.15	Alteració accidental de la informació	3	6	6	3	2			50%		20%			3,00		0,40
			E.18	Destrucció de la informació	3	6	6	3	2				100%	20%				3,00	0,40
			E.19	Fuga de informació	3	6	6	3	2		50%					3,00			
			A.4	Manipulació de la informació	3	6	6	3	2	50%	20%	20%		20%	1,50	1,20	1,20		0,40
			A.5	Suplantació d'identitat	3	6	6	3	2	100%	100%	20%			3,00	6,00	1,20		
			A.6	Abús de privilegis d'accés	3	6	6	3	2		20%	20%	20%			1,20	1,20	0,60	
			A.11	Accés no autoritzat	3	6	6	3	2		75%	5%				4,50	0,30		
			A.15	Modificació deliberada de la informació	3	6	6	3	2			75%					4,50		
			A.18	Destrucció de la informació	3	6	6	3	2				100%	20%				3,00	0,40
			A.19	Divulgació de informació	3	6	6	3	2		50%					3,00			
D.6	Codis font desenvolupament	M	E.1	Errors d'usuaris	5	8	8	6	4		5%	5%	5%			0,40	0,40	0,30	
			E.2	Erros d'administrador	5	8	8	6	4		100%	100%	100%			8,00	8,00	6,00	
			E.15	Alteració accidental de la informació	5	8	8	6	4			75%		20%			6,00		0,80
			E.18	Destrucció de la informació	5	8	8	6	4				100%	20%				6,00	0,80
			E.19	Fuga de informació	5	8	8	6	4		75%					6,00			

			A.4	Manipulació de la informació	5	8	8	6	4	50%	50%	20%		20%	2,50	4,00	1,60		0,80
			A.5	Suplantació d'identitat	5	8	8	6	4	100%	100%	20%			5,00	8,00	1,60		
			A.6	Abús de privilegis d'accés	5	8	8	6	4		20%	20%	20%			1,60	1,60	1,20	
			A.11	Accés no autoritzat	5	8	8	6	4		100%	5%				8,00	0,40		
			A.15	Modificació deliberada de la informació	5	8	8	6	4			100%					8,00		
			A.18	Destrucció de la informació	5	8	8	6	4				100%	20%				6,00	0,80
			A.19	Divulgació de informació	5	8	8	6	4		100%					8,00			
D.7	Registres	M	E.1	Errors d'usuaris	7	7	8	5	10		5%	5%	5%			0,35	0,40	0,25	
			E.2	Erros d'administrador	7	7	8	5	10		50%	100%	100%			3,50	8,00	5,00	
			E.15	Alteració accidental de la informació	7	7	8	5	10			75%		100%			6,00		10,00
			E.18	Destrucció de la informació	7	7	8	5	10				100%	100%				5,00	10,00
			E.19	Fuga de informació	7	7	8	5	10		50%					3,50			
			A.4	Manipulació de la informació	7	7	8	5	10	50%	50%	100%		100%	3,50	3,50	8,00		10,00
			A.5	Suplantació d'identitat	7	7	8	5	10	100%	20%	20%			7,00	1,40	1,60		
			A.6	Abús de privilegis d'accés	7	7	8	5	10		5%	5%	5%			0,35	0,40	0,25	
			A.11	Accés no autoritzat	7	7	8	5	10		50%	5%				3,50	0,40		
			A.15	Modificació deliberada de la informació	7	7	8	5	10			75%					6,00		
			A.18	Destrucció de la informació	7	7	8	5	10				100%	100%				5,00	10,00
			A.19	Divulgació de informació	7	7	8	5	10		75%					5,25			
D.8	videovigilància	B	E.1	Errors d'usuaris	3	6	6	3	1		5%	5%	5%			0,30	0,30	0,15	
			E.2	Erros d'administrador	3	6	6	3	1		100%	100%	100%			6,00	6,00	3,00	
			E.15	Alteració accidental de la informació	3	6	6	3	1			50%		75%			3,00		0,75
			E.18	Destrucció de la informació	3	6	6	3	1				100%	100%				3,00	1,00
			E.19	Fuga de informació	3	6	6	3	1		50%					3,00			
			A.4	Manipulació de la informació	3	6	6	3	1	50%	20%	20%		100%	1,50	1,20	1,20		1,00
			A.5	Suplantació d'identitat	3	6	6	3	1	20%	20%	20%			0,60	1,20	1,20		
			A.6	Abús de privilegis d'accés	3	6	6	3	1		20%	20%	20%			1,20	1,20	0,60	
			A.11	Accés no autoritzat	3	6	6	3	1		75%	5%				4,50	0,30		
			A.15	Modificació deliberada de la informació	3	6	6	3	1			75%					4,50		
			A.18	Destrucció de la informació	3	6	6	3	1				100%	100%				3,00	1,00
			A.19	Divulgació de informació	3	6	6	3	1		50%					3,00			

Taula 10. Valoració i Impacte actius de dades

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
KY.1	Certificats	A	E.1	Errors d'usuaris	10	10	10	5	6		50%	5%	75%			5,00	0,50	3,75	
			E.2	Erros d'administrador	10	10	10	5	6		50%	5%	100%			5,00	0,50	5,00	
			E.15	Alteració accidental de la informació	10	10	10	5	6			50%		20%			5,00		1,20
			E.18	Destrucció de la informació	10	10	10	5	6				100%	20%				5,00	1,20
			E.19	Fuga de informació	10	10	10	5	6		50%					5,00			
			A.5	Suplantació d'identitat	10	10	10	5	6	50%	50%	5%			5,00	5,00	0,50		
			A.6	Abús de privilegis d'accés	10	10	10	5	6		5%	5%	5%			0,50	0,50	0,25	
			A.11	Accés no autoritzat	10	10	10	5	6		50%	5%				5,00	0,50		
			A.15	Modificació deliberada de la informació	10	10	10	5	6			50%					5,00		
			A.18	Destrucció de la informació	10	10	10	5	6				100%	20%				5,00	1,20
			A.19	Divulgació de informació	10	10	10	5	6		50%					0,00			
KY.2	Claus d'encriptació portàtils	A	E.1	Errors d'usuaris	10	10	10	5	6		50%	5%	75%			5,00	0,50	3,75	
			E.2	Erros d'administrador	10	10	10	5	6		50%	5%	100%			5,00	0,50	5,00	
			E.15	Alteració accidental de la informació	10	10	10	5	6			50%		20%			5,00		1,20
			E.18	Destrucció de la informació	10	10	10	5	6				100%	20%				5,00	1,20
			E.19	Fuga de informació	10	10	10	5	6		50%					5,00			
			A.5	Suplantació d'identitat	10	10	10	5	6	50%	50%	5%			5,00	5,00	0,50		
			A.6	Abús de privilegis d'accés	10	10	10	5	6		5%	5%	5%			0,50	0,50	0,25	
			A.11	Accés no autoritzat	10	10	10	5	6		50%	5%				5,00	0,50		
			A.15	Modificació deliberada de la informació	10	10	10	5	6			50%					5,00		
			A.18	Destrucció de la informació	10	10	10	5	6				100%	20%				5,00	1,20
			A.19	Divulgació de informació	10	10	10	5	6		50%					0,00			

Taula 11. Valoració i Impacte actius de claus criptogràfiques

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
COM.1	Xarxa DMZ	MA	I.8	Fallada servei comunicacions	8	10	10	9	10				100%					9,00	
			E.2	Erros d'administrador	8	10	10	9	10		75%	75%	75%			7,50	7,50	6,75	
			E.15	Alteració accidental de la informació	8	10	10	9	10			50%		20%			5,00		2,00
			E.18	Destrucció de la informació	8	10	10	9	10				100%	20%				9,00	2,00
			E.19	Fuga de informació	8	10	10	9	10		100%					10,00			

			E.23	Errors manteniment o actualització d'equips	8	10	10	9	10				75%					6,75		
			E.24	Caiguda de sistema per esgotament de recursos	8	10	10	9	10				100%					9,00		
			A.5	Suplantació d'identitat	8	10	10	9	10	100%	75%	20%			8,00	7,50	2,00			
			A.6	Abús de privilegis d'accés	8	10	10	9	10		20%	20%	20%			2,00	2,00	1,80		
			A.7	Ús no previst	8	10	10	9	10		50%	20%	20%			5,00	2,00	1,80		
			A.11	Accés no autoritzat	8	10	10	9	10		100%	20%				10,00	2,00			
			A.15	Modificació deliberada de la informació	8	10	10	9	10			75%					7,50			
			A.19	Divulgació de informació	8	10	10	9	10		75%					7,50				
			A.24	Denegació de servei	8	10	10	9	10				100%					9,00		
COM.2	Accés Xarxa Pública	MB	I.8	Fallada servei comunicacions	1	1	1	1	1				100%					1,00		
			E.2	Erros d'administrador	1	1	1	1	1		5%	75%	75%			0,05	0,75	0,75		
			E.15	Alteració accidental de la informació	1	1	1	1	1			50%		20%			0,50		0,20	
			E.18	Destrucció de la informació	1	1	1	1	1				100%	20%				1,00	0,20	
			E.19	Fuga de informació	1	1	1	1	1		5%					0,05				
			E.23	Errors manteniment o actualització d'equips	1	1	1	1	1				75%					0,75		
			E.24	Caiguda de sistema per esgotament de recursos	1	1	1	1	1				100%					1,00		
			A.5	Suplantació d'identitat	1	1	1	1	1	5%	5%	20%			0,05	0,05	0,20			
			A.6	Abús de privilegis d'accés	1	1	1	1	1		5%	20%	20%			0,05	0,20	0,20		
			A.7	Ús no previst	1	1	1	1	1		5%	20%	20%			0,05	0,20	0,20		
			A.11	Accés no autoritzat	1	1	1	1	1		5%	20%				0,05	0,20			
			A.15	Modificació deliberada de la informació	1	1	1	1	1			75%					0,75			
			A.19	Divulgació de informació	1	1	1	1	1		5%					0,05				
			A.24	Denegació de servei	1	1	1	1	1				100%					1,00		
COM.3	Accés Xarxa Privada	MA	I.8	Fallada servei comunicacions	8	10	10	9	10				100%					9,00		
			E.2	Erros d'administrador	8	10	10	9	10		75%	75%	75%			7,50	7,50	6,75		
			E.15	Alteració accidental de la informació	8	10	10	9	10			50%		20%			5,00		2,00	
			E.18	Destrucció de la informació	8	10	10	9	10				100%	20%				9,00	2,00	
			E.19	Fuga de informació	8	10	10	9	10		100%					10,00				
			E.23	Errors manteniment o actualització d'equips	8	10	10	9	10				75%					6,75		
			E.24	Caiguda de sistema per esgotament de recursos	8	10	10	9	10				100%					9,00		
			A.5	Suplantació d'identitat	8	10	10	9	10	100%	100%	20%			8,00	10,00	2,00			
			A.6	Abús de privilegis d'accés	8	10	10	9	10		20%	20%	20%			2,00	2,00	1,80		
			A.7	Ús no previst	8	10	10	9	10		75%	20%	20%			7,50	2,00	1,80		
			A.11	Accés no autoritzat	8	10	10	9	10		100%	20%				10,00	2,00			

			A.15	Modificació deliberada de la informació	8	10	10	9	10			75%					7,50		
			A.19	Divulgació de informació	8	10	10	9	10		100%					10,00			
			A.24	Denegació de servei	8	10	10	9	10				100%					9,00	
COM.4	Xarxa Telefònica	M	I.8	Fallada servei comunicacions	4	5	3	3	4				100%					3,00	
			E.2	Erros d'administrador	4	5	3	3	4		5%	75%	100%			0,25	2,25	3,00	
			E.15	Alteració accidental de la informació	4	5	3	3	4			50%		20%			1,50		0,80
			E.18	Destrucció de la informació	4	5	3	3	4				100%	20%				3,00	0,80
			E.19	Fuga de informació	4	5	3	3	4		5%					0,25			
			E.23	Errors manteniment o actualització d'equips	4	5	3	3	4				100%					3,00	
			E.24	Caiguda de sistema per esgotament de recursos	4	5	3	3	4				100%					3,00	
			A.5	Suplantació d'identitat	4	5	3	3	4	50%	50%	20%			2,00	2,50	0,60		
			A.6	Abús de privilegis d'accés	4	5	3	3	4		5%	20%	20%			0,25	0,60	0,60	
			A.7	Ús no previst	4	5	3	3	4		5%	20%	20%			0,25	0,60	0,60	
			A.11	Accés no autoritzat	4	5	3	3	4		5%	20%				0,25	0,60		
			A.15	Modificació deliberada de la informació	4	5	3	3	4			75%					2,25		
			A.19	Divulgació de informació	4	5	3	3	4		5%					0,25			
			A.24	Denegació de servei	4	5	3	3	4				100%					3,00	

Taula 12. Valoració i Impacte actius de comunicació

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
S.1	Directori Actiu	MA	E.1	Errors d'usuaris	9	9	8	10	9		5%	5%	5%			0,45	0,40	0,50	
			E.2	Erros d'administrador	9	9	8	10	9		5%	20%	50%			0,45	0,45	5,00	
			E.15	Alteració accidental de la informació	9	9	8	10	9			50%		20%			4,00		1,80
			E.18	Destrucció de la informació	9	9	8	10	9				50%	20%				5,00	1,80
			E.19	Fuga de informació	9	9	8	10	9		5%					0,45			
			E.23	Errors manteniment o actualització d'equips	9	9	8	10	9				20%					2,00	
			E.24	Caiguda de sistema per esgotament de recursos	9	9	8	10	9				50%					5,00	
			A.5	Suplantació d'identitat	9	9	8	10	9	20%	20%	5%			1,80	1,80	0,40		
			A.6	Abús de privilegis d'accés	9	9	8	10	9		5%	5%	5%			0,45	0,40	0,50	
			A.7	Ús no previst	9	9	8	10	9		5%	5%	5%			0,45	0,40	0,50	
			A.11	Accés no autoritzat	9	9	8	10	9		20%	5%				1,80	0,40		
			A.15	Modificació deliberada de la informació	9	9	8	10	9			50%					4,00		
			A.18	Destrucció de la informació	9	9	8	10	9				50%	20%				5,00	1,80

			A.19	Divulgació de informació	9	9	8	10	9		5%					0,45			
			A.24	Denegació de servei	9	9	8	10	9				50%					5,00	
S.2	Web	M	E.1	Errors d'usuaris	6	3	8	7	6		5%	5%	5%			0,15	0,40	0,35	
			E.2	Erros d'administrador	6	3	8	7	6		50%	50%	75%			1,50	0,45	5,25	
			E.15	Alteració accidental de la informació	6	3	8	7	6			50%		20%			4,00		1,20
			E.18	Destrucció de la informació	6	3	8	7	6				75%	20%				5,25	1,20
			E.19	Fuga de informació	6	3	8	7	6		20%					0,60			
			E.23	Errors manteniment o actualització d'equips	6	3	8	7	6				75%					5,25	
			E.24	Caiguda de sistema per esgotament de recursos	6	3	8	7	6				100%					7,00	
			A.5	Suplantació d'identitat	6	3	8	7	6	20%	20%	20%			1,20	0,60	1,60		
			A.6	Abús de privilegis d'accés	6	3	8	7	6		20%	20%	20%			0,60	1,60	1,40	
			A.7	Ús no previst	6	3	8	7	6		20%	20%	20%			0,60	1,60	1,40	
			A.11	Accés no autoritzat	6	3	8	7	6		50%	20%				1,50	1,60		
			A.15	Modificació deliberada de la informació	6	3	8	7	6			50%					4,00		
			A.18	Destrucció de la informació	6	3	8	7	6				75%	20%				5,25	1,20
			A.19	Divulgació de informació	6	3	8	7	6		20%					0,60			
			A.24	Denegació de servei	6	3	8	7	6				100%					7,00	
S.3	Serveis al usuari final	MA	E.1	Errors d'usuaris	6	10	8	10	6		100%	50%	20%			10,00	4,00	2,00	
			E.2	Erros d'administrador	6	10	8	10	6		20%	20%	20%			2,00	0,45	2,00	
			E.15	Alteració accidental de la informació	6	10	8	10	6			75%		20%			6,00		1,20
			E.18	Destrucció de la informació	6	10	8	10	6				75%	50%				7,50	3,00
			E.19	Fuga de informació	6	10	8	10	6		100%					10,00			
			E.23	Errors manteniment o actualització d'equips	6	10	8	10	6				75%					7,50	
			E.24	Caiguda de sistema per esgotament de recursos	6	10	8	10	6				75%					7,50	
			A.5	Suplantació d'identitat	6	10	8	10	6	75%	50%	50%			4,50	5,00	4,00		
			A.6	Abús de privilegis d'accés	6	10	8	10	6		20%	20%	20%			2,00	1,60	2,00	
			A.7	Ús no previst	6	10	8	10	6		100%	20%	20%			10,00	1,60	2,00	
			A.11	Accés no autoritzat	6	10	8	10	6		100%	20%				10,00	1,60		
			A.15	Modificació deliberada de la informació	6	10	8	10	6			75%					6,00		
			A.18	Destrucció de la informació	6	10	8	10	6				75%	20%				7,50	1,20
			A.19	Divulgació de informació	6	10	8	10	6		100%					10,00			
			A.24	Denegació de servei	6	10	8	10	6				100%					10,00	
S.4	VPN	B	E.1	Errors d'usuaris	9	5	5	2	6		5%	5%	5%			0,25	0,25	0,10	
			E.2	Erros d'administrador	9	5	5	2	6		20%	20%	100%			1,00	0,45	2,00	

			E.15	Alteració accidental de la informació	9	5	5	2	6			20%		20%			1,00		1,20
			E.18	Destrucció de la informació	9	5	5	2	6				75%	20%				1,50	1,20
			E.19	Fuga de informació	9	5	5	2	6		75%					3,75			
			E.23	Errors manteniment o actualització d'equips	9	5	5	2	6				75%					1,50	
			E.24	Caiguda de sistema per esgotament de recursos	9	5	5	2	6				100%					2,00	
			A.5	Suplantació d'identitat	9	5	5	2	6	50%	75%	5%			4,50	3,75	0,25		
			A.6	Abús de privilegis d'accés	9	5	5	2	6		20%	20%	20%			1,00	1,00	0,40	
			A.7	Ús no previst	9	5	5	2	6		20%	20%	20%			1,00	1,00	0,40	
			A.11	Accés no autoritzat	9	5	5	2	6		100%	20%				5,00	1,00		
			A.15	Modificació deliberada de la informació	9	5	5	2	6			50%					2,50		
			A.18	Destrucció de la informació	9	5	5	2	6				75%	50%				1,50	3,00
			A.19	Divulgació de informació	9	5	5	2	6		100%					5,00			
			A.24	Denegació de servei	9	5	5	2	6				100%					2,00	
S.5	Intranet	MA	E.1	Errors d'usuaris	7	9	8	10	9		50%	5%	5%			4,50	0,40	0,50	
			E.2	Erros d'administrador	7	9	8	10	9		50%	50%	50%			4,50	0,45	5,00	
			E.15	Alteració accidental de la informació	7	9	8	10	9			50%		20%			4,00		1,80
			E.18	Destrucció de la informació	7	9	8	10	9				100%	20%				10,00	1,80
			E.19	Fuga de informació	7	9	8	10	9		100%					9,00			
			E.23	Errors manteniment o actualització d'equips	7	9	8	10	9				75%					7,50	
			E.24	Caiguda de sistema per esgotament de recursos	7	9	8	10	9				75%					7,50	
			A.5	Suplantació d'identitat	7	9	8	10	9	75%	100%	20%			5,25	9,00	1,60		
			A.6	Abús de privilegis d'accés	7	9	8	10	9		20%	20%	5%			1,80	1,60	0,50	
			A.7	Ús no previst	7	9	8	10	9		75%	20%	20%			6,75	1,60	2,00	
			A.11	Accés no autoritzat	7	9	8	10	9		100%	20%				9,00	1,60		
			A.15	Modificació deliberada de la informació	7	9	8	10	9			75%					6,00		
			A.18	Destrucció de la informació	7	9	8	10	9				50%	50%				5,00	4,50
			A.19	Divulgació de informació	7	9	8	10	9		75%					6,75			
			A.24	Denegació de servei	7	9	8	10	9				50%					5,00	
S.6	O365 (correu i fitxers)	B	E.1	Errors d'usuaris	3	3	3	3	3		75%	5%	5%			2,25	0,15	0,15	
			E.2	Erros d'administrador	3	3	3	3	3		20%	20%	75%			0,60	0,45	2,25	
			E.15	Alteració accidental de la informació	3	3	3	3	3			20%		5%			0,60		0,15
			E.18	Destrucció de la informació	3	3	3	3	3				50%	50%				1,50	1,50
			E.19	Fuga de informació	3	3	3	3	3		100%					3,00			
			E.23	Errors manteniment o actualització d'equips	3	3	3	3	3				50%					1,50	

			E.24	Caiguda de sistema per esgotament de recursos	3	3	3	3	3				100%					3,00	
			A.5	Suplantació d'identitat	3	3	3	3	3	100%	100%	20%			3,00	3,00	0,60		
			A.6	Abús de privilegis d'accés	3	3	3	3	3		20%	5%	5%			0,60	0,15	0,15	
			A.7	Ús no previst	3	3	3	3	3		20%	5%	5%			0,60	0,15	0,15	
			A.11	Accés no autoritzat	3	3	3	3	3		75%	20%				2,25	0,60		
			A.15	Modificació deliberada de la informació	3	3	3	3	3			20%					0,60		
			A.18	Destrucció de la informació	3	3	3	3	3				50%	20%				1,50	0,60
			A.19	Divulgació de informació	3	3	3	3	3		100%					3,00			
			A.24	Denegació de servei	3	3	3	3	3				100%					3,00	
S.7	Emmagatzematge de dades local	B	E.1	Errors d'usuaris	3	3	3	3	3		20%	20%	50%			0,60	0,60	1,50	
			E.2	Erros d'administrador	3	3	3	3	3		75%	50%	75%			2,25	0,45	2,25	
			E.15	Alteració accidental de la informació	3	3	3	3	3			75%		20%			2,25		0,60
			E.18	Destrucció de la informació	3	3	3	3	3				75%	20%				2,25	0,60
			E.19	Fuga de informació	3	3	3	3	3		100%					3,00			
			E.23	Errors manteniment o actualització d'equips	3	3	3	3	3				75%					2,25	
			E.24	Caiguda de sistema per esgotament de recursos	3	3	3	3	3				100%					3,00	
			A.5	Suplantació d'identitat	3	3	3	3	3	100%	100%	20%			3,00	3,00	0,60		
			A.6	Abús de privilegis d'accés	3	3	3	3	3		20%	20%	20%			0,60	0,60	0,60	
			A.7	Ús no previst	3	3	3	3	3		20%	20%	20%			0,60	0,60	0,60	
			A.11	Accés no autoritzat	3	3	3	3	3		100%	20%				3,00	0,60		
			A.15	Modificació deliberada de la informació	3	3	3	3	3			75%					2,25		
			A.18	Destrucció de la informació	3	3	3	3	3				75%	20%				2,25	0,60
			A.19	Divulgació de informació	3	3	3	3	3		100%					3,00			
			A.24	Denegació de servei	3	3	3	3	3				100%					3,00	

Taula 13. Valoració i Impacte actius de serveis

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
MED.1	Cabina de discs (emmagatzematge de xarxa)	MA	N.1	Foc	8	10	9	9	10				100%					9,00	
			N.2	Danys per aigua	8	10	9	9	10				100%					9,00	
			N.9	Origen meteorològic	8	10	9	9	10				100%					9,00	
			I.5	Averia d'origen físic o lògic	8	10	9	9	10				100%					9,00	
			I.6	Tall elèctric	8	10	9	9	10				100%					9,00	
			I.7	Condicions inadequades Temperatura o humitat	8	10	9	9	10				100%					9,00	

			I.10	Degradació dels suports d'emmagatzematge	8	10	9	9	10				75%					6,75	
			E.1	Errors d'usuaris	8	10	9	9	10		20%	20%	5%			2,00	1,80	0,45	
			E.2	Erros d'administrador	8	10	9	9	10		50%	20%	50%			5,00	1,80	4,50	
			E.15	Alteració accidental de la informació	8	10	9	9	10			75%		20%			6,75		2,00
			E.18	Destrucció de la informació	8	10	9	9	10				75%	20%				6,75	2,00
			E.19	Fuga de informació	8	10	9	9	10		100%					10,00			
			E.25	Pèrdua d'equips	8	10	9	9	10		20%		100%			2,00		9,00	
			A.7	Ús no previst	8	10	9	9	10		20%	5%	5%			2,00	0,45	0,45	
			A.11	Accés no autoritzat	8	10	9	9	10		75%	20%				7,50	1,80		
			A.15	Modificació deliberada de la informació	8	10	9	9	10			100%					9,00		
			A.18	Destrucció de la informació	8	10	9	9	10				100%	20%				9,00	2,00
			A.19	Divulgació de informació	8	10	9	9	10		20%					2,00			
			A.25	Robatori	8	10	9	9	10		75%		100%			7,50		9,00	

Taula 14. Valoració i Impacte actius de suports d'informació

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
AUX.1	Climatització CPD's	MA	N.1	Foc	1	1	9	10	1				100%					10,00	
			N.2	Danys per aigua	1	1	9	10	1				75%					7,50	
			N.9	Origen meteorològic	1	1	9	10	1				75%					7,50	
			I.5	Averia d'origen físic o lògic	1	1	9	10	1				75%					7,50	
			I.6	Tall elèctric	1	1	9	10	1				75%					7,50	
			I.7	Condicions inadequades Temperatura o humitat	1	1	9	10	1				75%					7,50	
			I.9	Interrupció d'altres serveis	1	1	9	10	1				20%					2,00	
			E.25	Pèrdua d'equips	1	1	9	10	1		5%		50%			0,05		5,00	
			A.7	Ús no previst	1	1	9	10	1		5%	50%	5%			0,05	4,50	0,50	
			A.11	Accés no autoritzat	1	1	9	10	1		5%	5%				0,05	0,45		
			A.25	Robatori	1	1	9	10	1		5%		50%			0,05		5,00	
AUX.2	Control de portes	M	N.1	Foc	5	8	7	6	5				100%					6,00	
			N.2	Danys per aigua	5	8	7	6	5				20%					1,20	
			N.9	Origen meteorològic	5	8	7	6	5				20%					1,20	
			I.5	Averia d'origen físic o lògic	5	8	7	6	5				50%					3,00	
			I.6	Tall elèctric	5	8	7	6	5				5%					0,30	
			I.7	Condicions inadequades Temperatura o humitat	5	8	7	6	5				5%					0,30	

			I.9	Interrupció d'altres serveis	5	8	7	6	5				5%					0,30	
			E.25	Pèrdua d'equips	5	8	7	6	5		5%		20%			0,40		1,20	
			A.7	Ús no previst	5	8	7	6	5		5%	5%	5%			0,40	0,35	0,30	
			A.11	Accés no autoritzat	5	8	7	6	5		75%	5%				6,00	0,35		
			A.25	Robatori	5	8	7	6	5		50%		20%			4,00		1,20	
AUX.3	Càmeres Seguretat	B	N.1	Foc	3	6	6	3	1				100%					3,00	
			N.2	Danys per aigua	3	6	6	3	1				50%					1,50	
			N.9	Origen meteorològic	3	6	6	3	1				50%					1,50	
			I.5	Averia d'origen físic o lògic	3	6	6	3	1				20%					0,60	
			I.6	Tall elèctric	3	6	6	3	1				20%					0,60	
			I.7	Condicions inadequades Temperatura o humitat	3	6	6	3	1				5%					0,15	
			I.9	Interrupció d'altres serveis	3	6	6	3	1				5%					0,15	
			E.25	Pèrdua d'equips	3	6	6	3	1		5%		20%			0,30		0,60	
			A.7	Ús no previst	3	6	6	3	1		75%	5%	20%			4,50	0,30	0,60	
			A.11	Accés no autoritzat	3	6	6	3	1		75%	5%				4,50	0,30		
			A.25	Robatori	3	6	6	3	1		5%		100%			0,30		3,00	
AUX.4	SAI 's	MA	N.1	Foc	1	1	10	10	1				100%					10,00	
			N.2	Danys per aigua	1	1	10	10	1				50%					5,00	
			N.9	Origen meteorològic	1	1	10	10	1				50%					5,00	
			I.5	Averia d'origen físic o lògic	1	1	10	10	1				50%					5,00	
			I.6	Tall elèctric	1	1	10	10	1				20%					2,00	
			I.7	Condicions inadequades Temperatura o humitat	1	1	10	10	1				20%					2,00	
			I.9	Interrupció d'altres serveis	1	1	10	10	1				5%					0,50	
			E.25	Pèrdua d'equips	1	1	10	10	1		5%		50%			0,05		5,00	
			A.7	Ús no previst	1	1	10	10	1		5%	20%	20%			0,05	2,00	2,00	
			A.11	Accés no autoritzat	1	1	10	10	1		5%	5%				0,05	0,50		
			A.25	Robatori	1	1	10	10	1		5%		50%			0,05		5,00	
AUX.5	Grup electrogen	B	N.1	Foc	1	1	8	9	1				100%					9,00	
			N.2	Danys per aigua	1	1	8	9	1				100%					9,00	
			N.9	Origen meteorològic	1	1	8	9	1				75%					6,75	
			I.5	Averia d'origen físic o lògic	1	1	8	9	1				75%					6,75	
			I.6	Tall elèctric	1	1	8	9	1				5%					0,45	
			I.7	Condicions inadequades Temperatura o humitat	1	1	8	9	1				20%					1,80	
			I.9	Interrupció d'altres serveis	1	1	8	9	1				50%					4,50	

			E.25	Pèrdua d'equips	1	1	8	9	1		5%		100%			0,05		9,00	
			A.7	Ús no previst	1	1	8	9	1		5%	5%	5%			0,05	0,40	0,45	
			A.11	Accés no autoritzat	1	1	8	9	1		5%	5%				0,05	0,40		
			A.25	Robatori	1	1	8	9	1		5%		100%			0,05		9,00	
AUX.6	Robot de cintes	MA	N.1	Foc	9	9	10	10	8				100%					10,00	
			N.2	Danys per aigua	9	9	10	10	8				100%					10,00	
			N.9	Origen meteorològic	9	9	10	10	8				100%					10,00	
			I.5	Averia d'origen físic o lògic	9	9	10	10	8				100%					10,00	
			I.6	Tall elèctric	9	9	10	10	8				100%					10,00	
			I.7	Condicions inadequades Temperatura o humitat	9	9	10	10	8				100%					10,00	
			I.9	Interrupció d'altres serveis	9	9	10	10	8				5%					0,50	
			E.25	Pèrdua d'equips	9	9	10	10	8		20%		100%			1,80		10,00	
			A.7	Ús no previst	9	9	10	10	8		5%	5%	5%			0,45	0,50	0,50	
			A.11	Accés no autoritzat	9	9	10	10	8		20%	5%				1,80	0,50		
			A.25	Robatori	9	9	10	10	8		50%		100%			4,50		10,00	
AUX.7	Mobiliari oficina	B	N.1	Foc	1	1	4	8	1				100%					8,00	
			N.2	Danys per aigua	1	1	4	8	1				75%					6,00	
			N.9	Origen meteorològic	1	1	4	8	1				20%					1,60	
			I.5	Averia d'origen físic o lògic	1	1	4	8	1				20%					1,60	
			I.6	Tall elèctric	1	1	4	8	1				5%					0,40	
			I.7	Condicions inadequades Temperatura o humitat	1	1	4	8	1				5%					0,40	
			I.9	Interrupció d'altres serveis	1	1	4	8	1				5%					0,40	
			E.25	Pèrdua d'equips	1	1	4	8	1		20%		75%			0,20		6,00	
			A.7	Ús no previst	1	1	4	8	1		5%	20%	5%			0,05	0,80	0,40	
			A.11	Accés no autoritzat	1	1	4	8	1		50%	5%				0,50	0,20		
			A.25	Robatori	1	1	4	8	1		5%		75%			0,05		6,00	

Taula 15. Valoració i Impacte actius d'equipament auxiliar

ID. Actiu	Actiu	Valor	ID. Amenaça	Amenaça	Valor					Degradació					Impacte				
					A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
P.1	Administradors	A	E.7	Deficiències amb la organització	6	10	7	6	3				50%					3,00	
			E.19	Fuga de informació	6	10	7	6	3		75%					7,50			
			E.28	Indisponiblitat del personal	6	10	7	6	3				50%					3,00	
			A.28	Indisponiblitat del personal	6	10	7	6	3				50%					3,00	

			A.29	Extorsió	6	10	7	6	3	75%	75%		5%		4,50	7,50		0,30	
			A.30	Enginyeria social	6	10	7	6	3	75%	75%		5%		4,50	7,50		0,30	
P.2	Programadors	A	E.7	Deficiències amb la organització	6	10	7	3	3				50%					1,50	
			E.19	Fuga de informació	6	10	7	3	3		75%					7,50			
			E.28	Indisponiblitat del personal	6	10	7	3	3				50%					1,50	
			A.28	Indisponiblitat del personal	6	10	7	3	3				50%					1,50	
			A.29	Extorsió	6	10	7	3	3	75%	75%		5%		4,50	7,50		0,15	
			A.30	Enginyeria social	6	10	7	3	3	50%	50%		5%		3,00	5,00		0,15	
P.3	Treballadors	A	E.7	Deficiències amb la organització	6	10	7	3	3				20%					0,60	
			E.19	Fuga de informació	6	10	7	3	3		100%					10,00			
			E.28	Indisponiblitat del personal	6	10	7	3	3				20%					0,60	
			A.28	Indisponiblitat del personal	6	10	7	3	3				20%					0,60	
			A.29	Extorsió	6	10	7	3	3	50%	75%		5%		3,00	7,50		0,15	
			A.30	Enginyeria social	6	10	7	3	3	75%	100%		5%		4,50	10,00		0,15	
P.4	Voluntaris	A	E.7	Deficiències amb la organització	6	10	7	3	3				5%					0,15	
			E.19	Fuga de informació	6	10	7	3	3		100%					10,00			
			E.28	Indisponiblitat del personal	6	10	7	3	3				5%					0,15	
			A.28	Indisponiblitat del personal	6	10	7	3	3				5%					0,15	
			A.29	Extorsió	6	10	7	3	3	50%	75%		5%		3,00	7,50		0,15	
			A.30	Enginyeria social	6	10	7	3	3	75%	100%		5%		4,50	10,00		0,15	
P.5	Proveïdors	A	E.7	Deficiències amb la organització	8	10	7	8	3				20%					1,60	
			E.19	Fuga de informació	8	10	7	8	3		75%					7,50			
			E.28	Indisponiblitat del personal	8	10	7	8	3				5%					0,40	

Taula 16. Valoració i Impacte actius d'actius de personal

4.2 Valoració del risc

ID. Actiu	Actiu	ID. Amenaça	Amenaça	Probabilitat					Impacte					RISC					Acció
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
L.1	Edificis	N.1	Foc				1					8,00					8,00		Assumir
		N.2	Danys per aigua				1					4,00					4,00		Assumir
		N.9	Origen meteorològic				2					0,40					0,80		Assumir
		A.7	Ús no previst		3	3	3			1,60	0,80	1,60			4,80	2,40	4,80		Assumir
		A.11	Accés no autoritzat		4	4				6,00	0,80				**24,00**	3,20			**Evitar**
L.2	CPDs	N.1	Foc				1					10,00					10,00		Assumir
		N.2	Danys per aigua				1					10,00					10,00		Assumir
		N.9	Origen meteorològic				1					0,50					0,50		Assumir
		A.7	Ús no previst		2	2	2			10,00	7,50	7,50			**20,00**	15,00	15,00		**Evitar**
		A.11	Accés no autoritzat		2	2				10,00	2,00				**20,00**	4,00			**Evitar**
L.3	Centre de Backup	N.1	Foc				1					9,00					9,00		Assumir
		N.2	Danys per aigua				1					4,50					4,50		Assumir
		N.9	Origen meteorològic				2					0,45					0,90		Assumir
		A.7	Ús no previst		3	3	3			1,80	1,80	1,80			5,40	5,40	5,40		Assumir
		A.11	Accés no autoritzat		4	4				5,00	1,80				**20,00**	7,20			**Evitar**

Taula 17. Risc instal·lacions

ID. Actiu	Actiu	ID. Amenaça	Amenaça	Probabilitat					Impacte					RISC					Acció
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
HW.1	Routers i Switchs	N.1	Foc				1					10,00					10,00		Assumir
		N.2	Danys per aigua				1					10,00					10,00		Assumir
		N.9	Origen meteorològic				1					10,00					10,00		Assumir
		I.5	Averia d'origen físic o lògic				1					10,00					10,00		Assumir
		I.6	Tall elèctric				1					10,00					10,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					10,00					10,00		Assumir
		E.2	Erros d'administrador		1	1	1			0,45	0,45	10,00			0,45	0,45	10,00		Assumir
		E.23	Errors manteniment o actualització d'equips				1					10,00					10,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				1					10,00					10,00		Assumir
		E.25	Pèrdua d'equips		1		1			1,80		10,00			1,80		10,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			1,80	1,80	2,00			1,80	1,80	2,00		Assumir

		A.7	Ús no previst		1	1	1			9,00	1,80	10,00			9,00	1,80	10,00		Assumir
		A.11	Accés no autoritzat		1	1				9,00	1,80				9,00	1,80			Assumir
		A.24	Denegació de servei				1					10,00					10,00		Assumir
		A.25	Robatori		1		1			1,80		10,00			1,80		10,00		Assumir
HW.2	Firewalls	N.1	Foc				1					10,00					10,00		Assumir
		N.2	Danys per aigua				1					10,00					10,00		Assumir
		N.9	Origen meteorològic				1					10,00					10,00		Assumir
		I.5	Averia d'origen físic o lògic				1					10,00					10,00		Assumir
		I.6	Tall elèctric				1					10,00					10,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					10,00					10,00		Assumir
		E.2	Erros d'administrador		1	1	1			0,45	0,45	10,00			0,45	0,45	10,00		Assumir
		E.23	Errors manteniment o actualització d'equips				1					10,00					10,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				1					10,00					10,00		Assumir
		E.25	Pèrdua d'equips		1		1			1,80		10,00			1,80		10,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			1,80	1,80	2,00			1,80	1,80	2,00		Assumir
		A.7	Ús no previst		1	1	1			9,00	1,80	10,00			9,00	1,80	10,00		Assumir
		A.11	Accés no autoritzat		1	1				9,00	1,80				9,00	1,80			Assumir
		A.24	Denegació de servei				1					10,00					10,00		Assumir
		A.25	Robatori		1		1			1,80		10,00			1,80		10,00		Assumir
HW.3	IDS/IPS	N.1	Foc				1					10,00					10,00		Assumir
		N.2	Danys per aigua				1					10,00					10,00		Assumir
		N.9	Origen meteorològic				1					10,00					10,00		Assumir
		I.5	Averia d'origen físic o lògic				1					10,00					10,00		Assumir
		I.6	Tall elèctric				1					10,00					10,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					10,00					10,00		Assumir
		E.2	Erros d'administrador		1	1	1			0,50	0,45	10,00			0,50	0,45	10,00		Assumir
		E.23	Errors manteniment o actualització d'equips				1					10,00					10,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				1					10,00					10,00		Assumir
		E.25	Pèrdua d'equips		1		1			2,00		10,00			2,00		10,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			2,00	1,80	2,00			2,00	1,80	2,00		Assumir
		A.7	Ús no previst		1	1	1			10,00	1,80	10,00			10,00	1,80	10,00		Assumir
		A.11	Accés no autoritzat		1	1				10,00	1,80				10,00	1,80			Assumir
		A.24	Denegació de servei				1					10,00					10,00		Assumir
		A.25	Robatori		1		1			2,00		10,00			2,00		10,00		Assumir

HW.4	AP's	N.1	Foc				1					3,00					3,00		Assumir
		N.2	Danys per aigua				1					3,00					3,00		Assumir
		N.9	Origen meteorològic				1					3,00					3,00		Assumir
		I.5	Averia d'origen físic o lògic				1					3,00					3,00		Assumir
		I.6	Tall elèctric				1					3,00					3,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					3,00					3,00		Assumir
		E.2	Erros d'administrador		1	1	1			0,15	0,15	3,00			0,15	0,15	3,00		Assumir
		E.23	Errors manteniment o actualització d'equips				1					3,00					3,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				1					3,00					3,00		Assumir
		E.25	Pèrdua d'equips		1		1			0,60		3,00			0,60		3,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			0,60	0,60	0,60			0,60	0,60	0,60		Assumir
		A.7	Ús no previst		1	1	1			3,00	0,60	3,00			3,00	0,60	3,00		Assumir
		A.11	Accés no autoritzat		1	1				3,00	0,60				3,00	0,60			Assumir
		A.24	Denegació de servei				1					3,00					3,00		Assumir
		A.25	Robatori		1		1			0,60		3,00			0,60		3,00		Assumir
HW.5	Servidors Producció	N.1	Foc				1					9,00					9,00		Assumir
		N.2	Danys per aigua				1					9,00					9,00		Assumir
		N.9	Origen meteorològic				1					9,00					9,00		Assumir
		I.5	Averia d'origen físic o lògic				1					9,00					9,00		Assumir
		I.6	Tall elèctric				1					9,00					9,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					9,00					9,00		Assumir
		E.2	Erros d'administrador		1	1	1			0,40	0,40	9,00			0,40	0,40	9,00		Assumir
		E.23	Errors manteniment o actualització d'equips				1					9,00					9,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				1					9,00					9,00		Assumir
		E.25	Pèrdua d'equips		1		1			1,60		9,00			1,60		9,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			1,60	1,60	9,00			1,60	1,60	9,00		Assumir
		A.7	Ús no previst		1	1	1			8,00	1,60	9,00			8,00	1,60	9,00		Assumir
		A.11	Accés no autoritzat		1	1				8,00	1,60				8,00	1,60			Assumir
		A.24	Denegació de servei				1					9,00					9,00		Assumir
		A.25	Robatori		1		1			1,60		9,00			1,60		9,00		Assumir
HW.6	Servidors Backup	N.1	Foc				1					10,00					10,00		Assumir
		N.2	Danys per aigua				1					10,00					10,00		Assumir
		N.9	Origen meteorològic				1					10,00					10,00		Assumir
		I.5	Averia d'origen físic o lògic				1					10,00					10,00		Assumir

		I.6	Tall elèctric				1					10,00					10,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					10,00					10,00		Assumir
		E.2	Erros d'administrador		1	1	1			0,40	0,40	10,00			0,40	0,40	10,00		Assumir
		E.23	Errors manteniment o actualització d'equips				1					10,00					10,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				1					10,00					10,00		Assumir
		E.25	Pèrdua d'equips		1		1			1,60		10,00			1,60		10,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			1,60	1,60	10,00			1,60	1,60	10,00		Assumir
		A.7	Ús no previst		1	1	1			8,00	1,60	10,00			8,00	1,60	10,00		Assumir
		A.11	Accés no autoritzat		1	1				8,00	1,60				8,00	1,60			Assumir
		A.24	Denegació de servei				1					10,00					10,00		Assumir
		A.25	Robatori		1		1			1,60		10,00			1,60		10,00		Assumir
HW.7	Servidors correu	N.1	Foc				1					3,00					3,00		Assumir
		N.2	Danys per aigua				2					3,00					6,00		Assumir
		N.9	Origen meteorològic				2					3,00					6,00		Assumir
		I.5	Averia d'origen físic o lògic				2					3,00					6,00		Assumir
		I.6	Tall elèctric				3					3,00					9,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					3,00					3,00		Assumir
		E.2	Erros d'administrador		1	1	1			0,15	0,15	3,00			0,15	0,15	3,00		Assumir
		E.23	Errors manteniment o actualització d'equips				1					3,00					3,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				2					3,00					6,00		Assumir
		E.25	Pèrdua d'equips		1		1			0,60		3,00			0,60		3,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			0,60	0,60	3,00			0,60	0,60	3,00		Assumir
		A.7	Ús no previst		1	1	1			3,00	0,60	3,00			3,00	0,60	3,00		Assumir
		A.11	Accés no autoritzat		1	1				3,00	0,60				3,00	0,60			Assumir
		A.24	Denegació de servei				1					3,00					3,00		Assumir
		A.25	Robatori		1		1			0,60		3,00			0,60		3,00		Assumir
HW.8	Entorn de proves	N.1	Foc				1					3,00					3,00		Assumir
		N.2	Danys per aigua				1					3,00					3,00		Assumir
		N.9	Origen meteorològic				1					3,00					3,00		Assumir
		I.5	Averia d'origen físic o lògic				1					3,00					3,00		Assumir
		I.6	Tall elèctric				1					3,00					3,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					3,00					3,00		Assumir
		E.2	Erros d'administrador		1	1	1			0,15	0,15	3,00			0,15	0,15	3,00		Assumir
		E.23	Errors manteniment o actualització d'equips				1					3,00					3,00		Assumir

		E.24	Caiguda de sistema per esgotament de recursos				1					3,00					3,00		Assumir
		E.25	Pèrdua d'equips		1		1			0,60		3,00			0,60		3,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			0,60	0,60	3,00			0,60	0,60	3,00		Assumir
		A.7	Ús no previst		1	1	1			3,00	0,60	3,00			3,00	0,60	3,00		Assumir
		A.11	Accés no autoritzat		1	1				3,00	0,60				3,00	0,60			Assumir
		A.24	Denegació de servei				1					3,00					3,00		Assumir
		A.25	Robatori		1		1			0,60		3,00			0,60		3,00		Assumir
HW.9	Telèfons IP	N.1	Foc				1					2,00					2,00		Assumir
		N.2	Danys per aigua				1					2,00					2,00		Assumir
		N.9	Origen meteorològic				1					2,00					2,00		Assumir
		I.5	Averia d'origen físic o lògic				1					2,00					2,00		Assumir
		I.6	Tall elèctric				1					2,00					2,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					2,00					2,00		Assumir
		E.2	Erros d'administrador		1	1	1			0,10	0,10	2,00			0,10	0,10	2,00		Assumir
		E.23	Errors manteniment o actualització d'equips				1					2,00					2,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				1					2,00					2,00		Assumir
		E.25	Pèrdua d'equips		1		1			0,40		2,00			0,40		2,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			0,40	0,40	0,40			0,40	0,40	0,40		Assumir
		A.7	Ús no previst		1	1	1			2,00	0,40	2,00			2,00	0,40	2,00		Assumir
		A.11	Accés no autoritzat		1	1				2,00	0,40				2,00	0,40			Assumir
		A.24	Denegació de servei				1					2,00					2,00		Assumir
		A.25	Robatori		1		1			0,40		2,00			0,40		2,00		Assumir
HW.10	Telèfons mòbils	N.1	Foc				1					4,00					4,00		Assumir
		N.2	Danys per aigua				4					4,00					**16,00**		**Reduir**
		N.9	Origen meteorològic				3					4,00					12,00		Assumir
		I.5	Averia d'origen físic o lògic				4					4,00					**16,00**		**Reduir**
		I.6	Tall elèctric				2					4,00					8,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				3					4,00					12,00		Assumir
		E.2	Erros d'administrador		2	2	2			0,40	0,20	4,00			0,80	0,40	8,00		Assumir
		E.23	Errors manteniment o actualització d'equips				3					4,00					12,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				3					4,00					12,00		Assumir
		E.25	Pèrdua d'equips		5		5			1,60		4,00			8,00		**20,00**		**Reduir**
		A.6	Abús de privilegis d'accés		2	2	2			1,60	0,80	0,80			3,20	1,60	1,60		Assumir
		A.7	Ús no previst		3	3	3			8,00	0,80	4,00			**24,00**	2,40	12,00		**Reduir**

		A.11	Accés no autoritzat		4	4				8,00	0,80				**32,00**	3,20			**Reduir**
		A.24	Denegació de servei				2					4,00					8,00		Assumir
		A.25	Robatori		4		4			1,60		4,00			6,40		**16,00**		**Reduir**
HW.11	Portàtils	N.1	Foc				1					4,00					4,00		Assumir
		N.2	Danys per aigua				1					4,00					4,00		Assumir
		N.9	Origen meteorològic				1					4,00					4,00		Assumir
		I.5	Averia d'origen físic o lògic				2					4,00					8,00		Assumir
		I.6	Tall elèctric				2					4,00					8,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					4,00					4,00		Assumir
		E.2	Erros d'administrador		2	2	2			0,40	0,20	4,00			0,80	0,40	8,00		Assumir
		E.23	Errors manteniment o actualització d'equips				2					4,00					8,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				2					4,00					8,00		Assumir
		E.25	Pèrdua d'equips		2		2			1,60		4,00			3,20		8,00		Assumir
		A.6	Abús de privilegis d'accés		1	1	1			1,60	0,80	0,80			1,60	0,80	0,80		Assumir
		A.7	Ús no previst		1	1	1			1,60	0,80	4,00			1,60	0,80	4,00		Assumir
		A.11	Accés no autoritzat		1	1				1,60	0,80				1,60	0,80			Assumir
		A.24	Denegació de servei				2					4,00					8,00		Assumir
		A.25	Robatori		2		2			1,60		4,00			3,20		8,00		Assumir
HW.12	PC's usuari i ús genèric	N.1	Foc				1					5,00					5,00		Assumir
		N.2	Danys per aigua				1					5,00					5,00		Assumir
		N.9	Origen meteorològic				1					5,00					5,00		Assumir
		I.5	Averia d'origen físic o lògic				2					5,00					10,00		Assumir
		I.6	Tall elèctric				2					5,00					10,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					5,00					5,00		Assumir
		E.2	Erros d'administrador		2	2	2			0,40	0,20	5,00			0,80	0,40	10,00		Assumir
		E.23	Errors manteniment o actualització d'equips				2					5,00					10,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				2					5,00					10,00		Assumir
		E.25	Pèrdua d'equips		1		1			1,60		5,00			1,60		5,00		Assumir
		A.6	Abús de privilegis d'accés		2	2	2			1,60	0,80	1,00			3,20	1,60	2,00		Assumir
		A.7	Ús no previst		1	1	1			1,60	0,80	5,00			1,60	0,80	5,00		Assumir
		A.11	Accés no autoritzat		1	1				1,60	0,80				1,60	0,80			Assumir
		A.24	Denegació de servei				2					5,00					10,00		Assumir
		A.25	Robatori		1		1			1,60		5,00			1,60		5,00		Assumir
HW.13	PC's accés públic	N.1	Foc				1					2,00					2,00		Assumir

		N.2	Danys per aigua				1					2,00					2,00		Assumir
		N.9	Origen meteorològic				1					2,00					2,00		Assumir
		I.5	Averia d'origen físic o lògic				2					2,00					4,00		Assumir
		I.6	Tall elèctric				2					2,00					4,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					2,00					2,00		Assumir
		E.2	Erros d'administrador		2	2	2			0,00	0,00	2,00			0,00	0,00	4,00		Assumir
		E.23	Errors manteniment o actualització d'equips				2					2,00					4,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				2					2,00					4,00		Assumir
		E.25	Pèrdua d'equips		1		1			0,00		2,00			0,00		2,00		Assumir
		A.6	Abús de privilegis d'accés		2	2	2			0,00	0,00	0,40			0,00	0,00	0,80		Assumir
		A.7	Ús no previst		1	1	1			0,00	0,00	2,00			0,00	0,00	2,00		Assumir
		A.11	Accés no autoritzat		1	1				0,00	0,00				0,00	0,00			Assumir
		A.24	Denegació de servei				2					2,00					4,00		Assumir
		A.25	Robatori		1		1			0,00		2,00			0,00		2,00		Assumir
HW.14	Impressores	N.1	Foc				1					4,00					4,00		Assumir
		N.2	Danys per aigua				3					4,00					12,00		Assumir
		N.9	Origen meteorològic				2					4,00					8,00		Assumir
		I.5	Averia d'origen físic o lògic				3					4,00					12,00		Assumir
		I.6	Tall elèctric				3					4,00					12,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				2					4,00					8,00		Assumir
		E.2	Erros d'administrador		3	3	3			0,25	0,20	4,00			0,75	0,60	12,00		Assumir
		E.23	Errors manteniment o actualització d'equips				3					4,00					12,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				4					4,00					**16,00**		**Reduir**
		E.25	Pèrdua d'equips		3		3			0,25		4,00			0,75		12,00		Assumir
		A.6	Abús de privilegis d'accés		4	4	4			0,25	0,20	0,80			1,00	0,80	3,20		Assumir
		A.7	Ús no previst		4	4	4			0,25	0,20	2,00			1,00	0,80	8,00		Assumir
		A.11	Accés no autoritzat		4	4				0,25	0,20				1,00	0,80			Assumir
		A.24	Denegació de servei				3					4,00					12,00		Assumir
		A.25	Robatori		2		2			0,25		4,00			0,50		8,00		Assumir
HW.15	Escàners	N.1	Foc				1					5,00					5,00		Assumir
		N.2	Danys per aigua				3					5,00					15,00		Assumir
		N.9	Origen meteorològic				2					5,00					10,00		Assumir
		I.5	Averia d'origen físic o lògic				3					5,00					15,00		Assumir
		I.6	Tall elèctric				3					5,00					15,00		Assumir

		I.7	Condicions inadequades Temperatura o humitat				2					5,00					10,00		Assumir
		E.2	Erros d'administrador		3	3	3			0,15	0,80	5,00			0,45	2,40	15,00		Assumir
		E.23	Errors manteniment o actualització d'equips				3					5,00					15,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				3					5,00					15,00		Assumir
		E.25	Pèrdua d'equips		3		3			3,00		5,00			9,00		15,00		Assumir
		A.6	Abús de privilegis d'accés		4	4	4			1,50	0,20	1,00			6,00	0,80	4,00		Assumir
		A.7	Ús no previst		4	4	4			3,00	0,80	2,50			12,00	3,20	10,00		Assumir
		A.11	Accés no autoritzat		4	4				3,00	0,80				12,00	3,20			Assumir
		A.24	Denegació de servei				3					5,00					15,00		Assumir
		A.25	Robatori		2		2			3,00		5,00			6,00		10,00		Assumir

Taula 18. Risc Hardware

ID. Actiu	Actiu	ID. Amenaça	Amenaça	Probabilitat					Impacte					RISC					Acció
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
SW.1	Plataforma corporativa	I.5	Averia d'origen físic o lògic				3					9,00					**27,00**		**Reduir**
		E.1	Errors d'usuaris		5	5	5			0,50	0,45	0,45			2,50	2,25	2,25		Assumir
		E.2	Erros d'administrador		3	3	3			5,00	4,50	4,50			15,00	13,50	13,50		Assumir
		E.8	Difusió de software maligne		3	3	3	3		10,00	9,00	9,00	5,00		**30,00**	**27,00**	**27,00**	15,00	**Reduir**
		E.15	Alteració accidental de la informació			5		5			1,80		0,50			9,00		2,50	Assumir
		E.18	Destrucció de la informació				4	4				9,00	7,50				**36,00**	**30,00**	**Reduir**
		E.19	Fuga de informació		3					10,00					**30,00**				**Evitar**
		E.20	Vulnerabilitat dels programes		3	3	3			2,00	4,50	0,45			6,00	13,50	1,35		Assumir
		E.21	Errors manteniment o actualització de programes			3	3				4,50	4,50				13,50	13,50		Assumir
		A.5	Suplantació d'identitat	5	5	5			8,00	10,00	0,45			**40,00**	**50,00**	2,25			**Evitar**
		A.6	Abús de privilegis d'accés		4	4	4			2,00	0,45	0,45			8,00	1,80	1,80		Assumir
		A.7	Ús no previst		3	3	3			0,50	0,45	0,45			1,50	1,35	1,35		Assumir
		A.8	Difusió de software maligne		3	3	3	3		10,00	0,45	0,45	5,00		**30,00**	1,35	1,35	15,00	**Reduir**
		A.11	Accés no autoritzat		4	4				10,00	1,80				**40,00**	7,20			**Evitar**
		A.15	Modificació deliberada de la informació			3					9,00					**27,00**			**Reduir**
		A.18	Destrucció de la informació				4	4				9,00	7,50				**36,00**	**30,00**	**Reduir**
		A.19	Divulgació de informació		3					10,00					**30,00**				**Reduir**
SW.2	Gestor Base de Dades	I.5	Averia d'origen físic o lògic				3					9,00					**27,00**		**Reduir**
		E.1	Errors d'usuaris		5	5	5			0,50	0,45	0,45			2,50	2,25	2,25		Assumir
		E.2	Erros d'administrador		3	3	3			5,00	4,50	4,50			15,00	13,50	13,50		Assumir

		E.8	Difusió de software maligne		3	3	3	3		10,00	9,00	9,00	5,00		**30,00**	**27,00**	**27,00**	15,00	**Reduir**
		E.15	Alteració accidental de la informació			5		5			1,80		0,50			9,00		2,50	Assumir
		E.18	Destrucció de la informació				4	4				9,00	7,50				**36,00**	**30,00**	**Reduir**
		E.19	Fuga de informació		3					10,00					**30,00**				**Evitar**
		E.20	Vulnerabilitat dels programes		3	3	3			2,00	4,50	0,45			6,00	13,50	1,35		Assumir
		E.21	Errors manteniment o actualització de programes			3	3				4,50	4,50				13,50	13,50		Assumir
		A.5	Suplantació d'identitat	5	5	5			8,00	10,00	0,45			**40,00**	**50,00**	2,25			**Evitar**
		A.6	Abús de privilegis d'accés		4	4	4			2,00	0,45	0,45			8,00	1,80	1,80		Assumir
		A.7	Ús no previst		3	3	3			0,50	0,45	0,45			1,50	1,35	1,35		Assumir
		A.8	Difusió de software maligne		3	3	3	3		10,00	0,45	0,45	5,00		**30,00**	1,35	1,35	15,00	**Reduir**
		A.11	Accés no autoritzat		4	4				10,00	1,80				**40,00**	7,20			**Evitar**
		A.15	Modificació deliberada de la informació			3					9,00					**27,00**			**Reduir**
		A.18	Destrucció de la informació				4	4				9,00	7,50				**36,00**	**30,00**	**Reduir**
		A.19	Divulgació de informació		3					10,00					**30,00**				**Reduir**
SW.3	Office 365 corp	I.5	Averia d'origen físic o lògic				4					3,00					12,00		Assumir
		E.1	Errors d'usuaris		5	5	5			0,15	0,15	0,15			0,75	0,75	0,75		Assumir
		E.2	Erros d'administrador		3	3	3			1,50	1,50	1,50			4,50	4,50	4,50		Assumir
		E.8	Difusió de software maligne		4	4	4	4		3,00	3,00	3,00	2,00		12,00	12,00	12,00	8,00	Assumir
		E.15	Alteració accidental de la informació			4		4			0,60		0,15			2,40		0,60	Assumir
		E.18	Destrucció de la informació				5	5				3,00	2,25				15,00	11,25	Assumir
		E.19	Fuga de informació		4					3,00					12,00				Assumir
		E.20	Vulnerabilitat dels programes		3	3	3			0,60	1,50	0,15			1,80	4,50	0,45		Assumir
		E.21	Errors manteniment o actualització de programes			3	3				1,50	1,50				4,50	4,50		Assumir
		A.5	Suplantació d'identitat	4	4	4			3,00	3,00	0,15			12,00	12,00	0,60			Assumir
		A.6	Abús de privilegis d'accés		4	4	4			0,60	0,15	0,15			2,40	0,60	0,60		Assumir
		A.7	Ús no previst		3	3	3			0,15	0,15	0,15			0,45	0,45	0,45		Assumir
		A.8	Difusió de software maligne		4	4	4	4		3,00	0,15	0,15	1,50		12,00	0,60	0,60	6,00	Assumir
		A.11	Accés no autoritzat		4	4				3,00	0,60				12,00	2,40			Assumir
		A.15	Modificació deliberada de la informació			3					3,00					9,00			Assumir
		A.18	Destrucció de la informació				4	4				3,00	2,25				12,00	9,00	Assumir
		A.19	Divulgació de informació		4					3,00					12,00				Assumir
SW.4	Antivirus	I.5	Averia d'origen físic o lògic				3					10,00					**30,00**		**Derivar**
		E.1	Errors d'usuaris		3	3	3			0,30	0,50	0,50			0,90	1,50	1,50		Assumir
		E.2	Erros d'administrador		3	3	3			3,00	5,00	5,00			9,00	15,00	15,00		Assumir

		E.8	Difusió de software maligne		4	4	4	4		6,00	10,00	10,00	5,00		**24,00**	**40,00**	**40,00**	**20,00**	**Derivar**
		E.15	Alteració accidental de la informació			3		3			2,00		0,50			6,00		1,50	Assumir
		E.18	Destrucció de la informació				3	3				10,00	7,50				**30,00**	**22,50**	**Derivar**
		E.19	Fuga de informació		3					6,00					**18,00**				**Derivar**
		E.20	Vulnerabilitat dels programes		4	4	4			1,20	5,00	0,50			4,80	**20,00**	2,00		**Derivar**
		E.21	Errors manteniment o actualització de programes			5	5				5,00	5,00				**25,00**	**25,00**		**Derivar**
		A.5	Suplantació d'identitat	3	3	3			6,00	6,00	0,50			**18,00**	**18,00**	1,50			**Derivar**
		A.6	Abús de privilegis d'accés		3	3	3			1,20	0,50	0,50			3,60	1,50	1,50		Assumir
		A.7	Ús no previst		3	3	3			0,30	0,50	0,50			0,90	1,50	1,50		Assumir
		A.8	Difusió de software maligne		2	2	2	2		6,00	0,50	0,50	5,00		12,00	1,00	1,00	10,00	Assumir
		A.11	Accés no autoritzat		2	2				6,00	2,00				12,00	4,00			Assumir
		A.15	Modificació deliberada de la informació			3					10,00					**30,00**			**Derivar**
		A.18	Destrucció de la informació				3	3				10,00	7,50				**30,00**	**22,50**	**Derivar**
		A.19	Divulgació de informació		2					6,00					12,00				Assumir
SW.5	Sistemes operatius	I.5	Averia d'origen físic o lògic				4					1,00					4,00		Assumir
		E.1	Errors d'usuaris		4	4	4			0,05	0,05	0,05			0,20	0,20	0,20		Assumir
		E.2	Erros d'administrador		3	3	3			0,50	0,50	0,50			1,50	1,50	1,50		Assumir
		E.8	Difusió de software maligne		3	3	3	3		1,00	1,00	1,00	1,00		3,00	3,00	3,00	3,00	Assumir
		E.15	Alteració accidental de la informació			3		3			0,20		0,05			0,60		0,15	Assumir
		E.18	Destrucció de la informació				3	3				1,00	0,75				3,00	2,25	Assumir
		E.19	Fuga de informació		3					1,00					3,00				Assumir
		E.20	Vulnerabilitat dels programes		4	4	4			0,20	0,50	0,05			0,80	2,00	0,20		Assumir
		E.21	Errors manteniment o actualització de programes			5	5				0,50	0,50				2,50	2,50		Assumir
		A.5	Suplantació d'identitat	5	5	5			1,00	1,00	0,05			5,00	5,00	0,25			Assumir
		A.6	Abús de privilegis d'accés		5	5	5			0,20	0,05	0,05			1,00	0,25	0,25		Assumir
		A.7	Ús no previst		5	5	5			0,05	0,05	0,05			0,25	0,25	0,25		Assumir
		A.8	Difusió de software maligne		4	4	4	4		1,00	0,05	0,05	0,50		4,00	0,20	0,20	2,00	Assumir
		A.11	Accés no autoritzat		4	4				1,00	0,20				4,00	0,80			Assumir
		A.15	Modificació deliberada de la informació			3					1,00					3,00			Assumir
		A.18	Destrucció de la informació				4	4				1,00	0,75				4,00	3,00	Assumir
		A.19	Divulgació de informació		3					1,00					3,00				Assumir

Taula 19. Risc Software

ID. Actiu	Actiu		Amenaça	Probabilitat	Impacte	RISC	Acció

		ID. Amenaça		A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
D.1	Fitxers personals	E.1	Errors d'usuaris		5	5	5			9,00	4,00	3,00			**45,00**	**20,00**	15,00		**Reduir**
		E.2	Erros d'administrador		1	1	1			9,00	8,00	6,00			9,00	8,00	6,00		Assumir
		E.15	Alteració accidental de la informació			5		5			1,60		1,20			8,00		6,00	Assumir
		E.18	Destrucció de la informació				4	4				6,00	1,20				**24,00**	4,80	**Reduir**
		E.19	Fuga de informació		4					9,00					**36,00**				**Evitar**
		A.4	Manipulació de la informació	3	3	3		3	5,00	9,00	8,00		1,20	15,00	**27,00**	**24,00**		3,60	**Reduir**
		A.5	Suplantació d'identitat	5	5	5			5,00	9,00	1,60			**25,00**	**45,00**	8,00			**Evitar**
		A.6	Abús de privilegis d'accés		4	4	4			1,80	1,60	1,20			7,20	6,40	4,80		Assumir
		A.11	Accés no autoritzat		4	4				9,00	1,60				**36,00**	6,40			**Evitar**
		A.15	Modificació deliberada de la informació			3					8,00					**24,00**			**Reduir**
		A.18	Destrucció de la informació				4	4				6,00	1,20				**24,00**	4,80	**Reduir**
		A.19	Divulgació de informació		4					9,00					**36,00**				**Reduir**
D.2	Bases de dades Aplicacions	E.1	Errors d'usuaris		5	5	5			10,00	5,00	4,00			**50,00**	**25,00**	**20,00**		**Reduir**
		E.2	Erros d'administrador		1	1	1			10,00	10,00	8,00			10,00	10,00	8,00		Assumir
		E.15	Alteració accidental de la informació			5		5			2,00		1,80			10,00		9,00	Assumir
		E.18	Destrucció de la informació				4	4				8,00	1,80				**32,00**	7,20	**Reduir**
		E.19	Fuga de informació		4					10,00					**40,00**				**Evitar**
		A.4	Manipulació de la informació	3	3	3		3	8,00	10,00	10,00		1,80	**24,00**	**30,00**	**30,00**		5,40	**Reduir**
		A.5	Suplantació d'identitat	5	5	5			8,00	10,00	2,00			**40,00**	**50,00**	10,00			**Evitar**
		A.6	Abús de privilegis d'accés		4	4	4			2,00	2,00	1,60			8,00	8,00	6,40		Assumir
		A.11	Accés no autoritzat		4	4				10,00	2,00				**40,00**	8,00			**Evitar**
		A.15	Modificació deliberada de la informació			3					10,00					**30,00**			**Reduir**
		A.18	Destrucció de la informació				3	3				8,00	1,80				**24,00**	5,40	**Reduir**
		A.19	Divulgació de informació		3					10,00					**30,00**				**Reduir**
D.3	Copies de Seguretat	E.1	Errors d'usuaris		3	3	3			4,00	5,00	6,00			12,00	15,00	**18,00**		**Reduir**
		E.2	Erros d'administrador		2	2	2			8,00	10,00	6,00			**16,00**	**20,00**	12,00		**Reduir**
		E.15	Alteració accidental de la informació			2		2			10,00		0,80			**20,00**		1,60	**Reduir**
		E.18	Destrucció de la informació				3	3				6,00	0,80				**18,00**	2,40	**Reduir**
		E.19	Fuga de informació		2					8,00					**16,00**				**Evitar**
		A.4	Manipulació de la informació	2	2	2		2	4,00	6,00	10,00		0,80	8,00	12,00	**20,00**		1,60	**Reduir**
		A.5	Suplantació d'identitat	2	2	2			4,00	8,00	2,00			8,00	**16,00**	4,00			**Evitar**
		A.6	Abús de privilegis d'accés		2	2	2			1,60	2,00	1,20			3,20	4,00	2,40		Assumir
		A.11	Accés no autoritzat		2	2				8,00	0,50				**16,00**	1,00			**Evitar**

		A.15	Modificació deliberada de la informació			2					10,00						**20,00**			**Reduir**
		A.18	Destrucció de la informació				3	3				6,00	0,80					**18,00**	2,40	**Reduir**
		A.19	Divulgació de informació		2					8,00					**16,00**					**Reduir**
D.4	Bases de dades Gestió interna	E.1	Errors d'usuaris		5	5	5			6,00	3,00	1,50			**30,00**	15,00	7,50		**Reduir**
		E.2	Erros d'administrador		1	1	1			6,00	6,00	3,00			6,00	6,00	3,00		Assumir
		E.15	Alteració accidental de la informació			5		5			1,20		1,20			6,00		6,00	Assumir
		E.18	Destrucció de la informació				4	4				3,00	1,20				12,00	4,80	Assumir
		E.19	Fuga de informació		4					6,00					**24,00**				**Evitar**
		A.4	Manipulació de la informació	3	3	3		3	6,00	6,00	6,00		1,20	**18,00**	**18,00**	**18,00**		3,60	**Reduir**
		A.5	Suplantació d'identitat	5	5	5			6,00	6,00	1,20			**30,00**	**30,00**	6,00			**Evitar**
		A.6	Abús de privilegis d'accés		4	4	4			1,20	1,20	0,60			4,80	4,80	2,40		Assumir
		A.11	Accés no autoritzat		4	4				6,00	1,20				**24,00**	4,80			**Evitar**
		A.15	Modificació deliberada de la informació			3					6,00					**18,00**			**Reduir**
		A.18	Destrucció de la informació				3	3				3,00	1,20				9,00	3,60	**Reduir**
		A.19	Divulgació de informació		3					6,00					**18,00**				**Reduir**
D.5	Dades control accés	E.1	Errors d'usuaris		3	3	3			3,00	6,00	3,00			9,00	**18,00**	9,00		**Reduir**
		E.2	Erros d'administrador		2	2	2			6,00	6,00	3,00			12,00	12,00	6,00		Assumir
		E.15	Alteració accidental de la informació			2		2			3,00		0,40			6,00		0,80	Assumir
		E.18	Destrucció de la informació				2	2				3,00	0,40				6,00	0,80	Assumir
		E.19	Fuga de informació		2					3,00					6,00				Assumir
		A.4	Manipulació de la informació	2	2	2		2	1,50	1,20	1,20		0,40	3,00	2,40	2,40		0,80	Assumir
		A.5	Suplantació d'identitat	2	2	2			3,00	6,00	1,20			6,00	12,00	2,40			Assumir
		A.6	Abús de privilegis d'accés		2	2	2			1,20	1,20	0,60			2,40	2,40	1,20		Assumir
		A.11	Accés no autoritzat		2	2				4,50	0,30				9,00	0,60			Assumir
		A.15	Modificació deliberada de la informació			2					4,50					9,00			Assumir
		A.18	Destrucció de la informació				2	2				3,00	0,40				6,00	0,80	Assumir
		A.19	Divulgació de informació		2					3,00					6,00				Assumir
D.6	Codis font desenvolupament	E.1	Errors d'usuaris		2	2	2			0,40	0,40	0,30			0,80	0,80	0,60		Assumir
		E.2	Erros d'administrador		3	3	3			8,00	8,00	6,00			**24,00**	**24,00**	**18,00**		**Reduir**
		E.15	Alteració accidental de la informació			2		2			6,00		0,80			12,00		1,60	Assumir
		E.18	Destrucció de la informació				2	2				6,00	0,80				12,00	1,60	Assumir
		E.19	Fuga de informació		2					6,00					12,00				Assumir
		A.4	Manipulació de la informació	2	2	2		2	2,50	4,00	1,60		0,80	5,00	8,00	3,20		1,60	Assumir
		A.5	Suplantació d'identitat	2	2	2			5,00	8,00	1,60			10,00	**16,00**	3,20			**Evitar**

		A.6	Abús de privilegis d'accés		3	3	3			1,60	1,60	1,20			4,80	4,80	3,60		Assumir
		A.11	Accés no autoritzat		2	2				8,00	0,40				**16,00**	0,80			**Evitar**
		A.15	Modificació deliberada de la informació			2					8,00					**16,00**			**Reduir**
		A.18	Destrucció de la informació				2	2				6,00	0,80				12,00	1,60	**Reduir**
		A.19	Divulgació de informació		2					8,00					**16,00**				**Reduir**
D.7	Registres	E.1	Errors d'usuaris		2	2	2			0,35	0,40	0,25			0,70	0,80	0,50		Assumir
		E.2	Erros d'administrador		2	2	2			3,50	8,00	5,00			7,00	**16,00**	10,00		**Reduir**
		E.15	Alteració accidental de la informació			2		2			6,00		10,00			12,00		**20,00**	**Reduir**
		E.18	Destrucció de la informació				2	2				5,00	10,00				10,00	**20,00**	**Reduir**
		E.19	Fuga de informació		2					3,50					7,00				Assumir
		A.4	Manipulació de la informació	2	2	2		2	3,50	3,50	8,00		10,00	7,00	7,00	**16,00**		**20,00**	**Reduir**
		A.5	Suplantació d'identitat	2	2	2			7,00	1,40	1,60			14,00	2,80	3,20			Assumir
		A.6	Abús de privilegis d'accés		2	2	2			0,35	0,40	0,25			0,70	0,80	0,50		Assumir
		A.11	Accés no autoritzat		2	2				3,50	0,40				7,00	0,80			Assumir
		A.15	Modificació deliberada de la informació			2					6,00					12,00			Assumir
		A.18	Destrucció de la informació				2	2				5,00	10,00				10,00	**20,00**	**Reduir**
		A.19	Divulgació de informació		2					5,25					10,50				Assumir
D.8	videovigilància	E.1	Errors d'usuaris		3	3	3			0,30	0,30	0,15			0,90	0,90	0,45		Assumir
		E.2	Erros d'administrador		2	2	2			6,00	6,00	3,00			12,00	12,00	6,00		Assumir
		E.15	Alteració accidental de la informació			2		2			3,00		0,75			6,00		1,50	Assumir
		E.18	Destrucció de la informació				2	2				3,00	1,00				6,00	2,00	Assumir
		E.19	Fuga de informació		2					3,00					6,00				Assumir
		A.4	Manipulació de la informació	2	2	2		2	1,50	1,20	1,20		1,00	3,00	2,40	2,40		2,00	Assumir
		A.5	Suplantació d'identitat	2	2	2			0,60	1,20	1,20			1,20	2,40	2,40			Assumir
		A.6	Abús de privilegis d'accés		2	2	2			1,20	1,20	0,60			2,40	2,40	1,20		Assumir
		A.11	Accés no autoritzat		2	2				4,50	0,30				9,00	0,60			Assumir
		A.15	Modificació deliberada de la informació			2					4,50					9,00			Assumir
		A.18	Destrucció de la informació				2	2				3,00	1,00				6,00	2,00	Assumir
		A.19	Divulgació de informació		2					3,00					6,00				Assumir

Taula 20. Risc dades

ID. Actiu	Actiu	ID. Amenaça	Amenaça	Probabilitat					Impacte					RISC					Acció
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
KY.1	Certificats	E.1	Errors d'usuaris		3	3	3			5,00	0,50	3,75			15,00	1,50	11,25		Assumir

		E.2	Erros d'administrador		2	2	2			5,00	0,50	5,00			10,00	1,00	10,00		Assumir
		E.15	Alteració accidental de la informació			2		2			5,00		1,20			10,00		2,40	Assumir
		E.18	Destrucció de la informació				2	2				5,00	1,20				10,00	2,40	Assumir
		E.19	Fuga de informació		2					5,00					10,00				Assumir
		A.5	Suplantació d'identitat	2	2	2			5,00	5,00	0,50			10,00	10,00	1,00			Assumir
		A.6	Abús de privilegis d'accés		2	2	2			0,50	0,50	0,25			1,00	1,00	0,50		Assumir
		A.11	Accés no autoritzat		2	2				5,00	0,50				10,00	1,00			Assumir
		A.15	Modificació deliberada de la informació			2					5,00					10,00			Assumir
		A.18	Destrucció de la informació				2	2				5,00	1,20				10,00	2,40	Assumir
		A.19	Divulgació de informació		2					0,00					0,00				Assumir
KY.2	Claus d'encriptació portàtils	E.1	Errors d'usuaris		3	3	3			5,00	0,50	3,75			15,00	1,50	11,25		Assumir
		E.2	Erros d'administrador		2	2	2			5,00	0,50	5,00			10,00	1,00	10,00		Assumir
		E.15	Alteració accidental de la informació			2		2			5,00		1,20			10,00		2,40	Assumir
		E.18	Destrucció de la informació				2	2				5,00	1,20				10,00	2,40	Assumir
		E.19	Fuga de informació		2					5,00					10,00				Assumir
		A.5	Suplantació d'identitat	2	2	2			5,00	5,00	0,50			10,00	10,00	1,00			Assumir
		A.6	Abús de privilegis d'accés		2	2	2			0,50	0,50	0,25			1,00	1,00	0,50		Assumir
		A.11	Accés no autoritzat		2	2				5,00	0,50				10,00	1,00			Assumir
		A.15	Modificació deliberada de la informació			2					5,00					10,00			Assumir
		A.18	Destrucció de la informació				2	2				5,00	1,20				10,00	2,40	Assumir
		A.19	Divulgació de informació		2					0,00					0,00				Assumir

Taula 21. Risc claus criptogràfiques

ID. Actiu	Actiu	ID. Amenaça	Amenaça	Probabilitat					Impacte					RISC					Acció
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
COM.1	Xarxa DMZ	I.8	Fallada servei comunicacions				3					9,00					**27,00**		**Reduir**
		E.2	Erros d'administrador		3	3	3			7,50	7,50	6,75			**22,50**	**22,50**	**20,25**		**Reduir**
		E.15	Alteració accidental de la informació			3		3			5,00		2,00			15,00		6,00	Assumir
		E.18	Destrucció de la informació				2	2				9,00	2,00				**18,00**	4,00	**Reduir**
		E.19	Fuga de informació		2					10,00					**20,00**				**Evitar**
		E.23	Errors manteniment o actualització d'equips				3					6,75					**20,25**		**Reduir**
		E.24	Caiguda de sistema per esgotament de recursos				2					9,00					**18,00**		**Reduir**
		A.5	Suplantació d'identitat	5	5	5			8,00	7,50	2,00			**40,00**	**37,50**	10,00			**Evitar**
		A.6	Abús de privilegis d'accés		3	3	3			2,00	2,00	1,80			6,00	6,00	5,40		Assumir

		A.7	Ús no previst		3	3	3			5,00	2,00	1,80			15,00	6,00	5,40		Assumir
		A.11	Accés no autoritzat		2	2				10,00	2,00				**20,00**	4,00			**Evitar**
		A.15	Modificació deliberada de la informació			2					7,50					15,00			Assumir
		A.19	Divulgació de informació		2					7,50					15,00				Assumir
		A.24	Denegació de servei				2					9,00					**18,00**		**Reduir**
COM.2	Accés Xarxa Pública	I.8	Fallada servei comunicacions				3					1,00					3,00		Assumir
		E.2	Erros d'administrador		3	3	3			0,05	0,75	0,75			0,15	2,25	2,25		Assumir
		E.15	Alteració accidental de la informació			4		4			0,50		0,20			2,00		0,80	Assumir
		E.18	Destrucció de la informació				4	4				1,00	0,20				4,00	0,80	Assumir
		E.19	Fuga de informació		5					0,05					0,25				Assumir
		E.23	Errors manteniment o actualització d'equips				4					0,75					3,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				4					1,00					4,00		Assumir
		A.5	Suplantació d'identitat	5	5	5			0,05	0,05	0,20			0,25	0,25	1,00			Assumir
		A.6	Abús de privilegis d'accés		3	3	3			0,05	0,20	0,20			0,15	0,60	0,60		Assumir
		A.7	Ús no previst		5	5	5			0,05	0,20	0,20			0,25	1,00	1,00		Assumir
		A.11	Accés no autoritzat		4	4				0,05	0,20				0,20	0,80			Assumir
		A.15	Modificació deliberada de la informació			4					0,75					3,00			Assumir
		A.19	Divulgació de informació		5					0,05					0,25				Assumir
		A.24	Denegació de servei				4					1,00					4,00		Assumir
COM.3	Accés Xarxa Privada	I.8	Fallada servei comunicacions				3					9,00					**27,00**		**Reduir**
		E.2	Erros d'administrador		3	3	3			7,50	7,50	6,75			**22,50**	**22,50**	**20,25**		**Reduir**
		E.15	Alteració accidental de la informació			3		3			5,00		2,00			15,00		6,00	Assumir
		E.18	Destrucció de la informació				2	2				9,00	2,00				**18,00**	4,00	**Reduir**
		E.19	Fuga de informació		3					10,00					**30,00**				**Evitar**
		E.23	Errors manteniment o actualització d'equips				3					6,75					**20,25**		**Reduir**
		E.24	Caiguda de sistema per esgotament de recursos				2					9,00					**18,00**		**Reduir**
		A.5	Suplantació d'identitat	5	5	5			8,00	10,00	2,00			**40,00**	**50,00**	10,00			**Evitar**
		A.6	Abús de privilegis d'accés		3	3	3			2,00	2,00	1,80			6,00	6,00	5,40		Assumir
		A.7	Ús no previst		3	3	3			7,50	2,00	1,80			**22,50**	6,00	5,40		**Evitar**
		A.11	Accés no autoritzat		3	3				10,00	2,00				**30,00**	6,00			**Evitar**
		A.15	Modificació deliberada de la informació			2					7,50					15,00			Assumir
		A.19	Divulgació de informació		3					10,00					**30,00**				**Reduir**
		A.24	Denegació de servei				3					9,00					**27,00**		**Reduir**
COM.4	Xarxa Telefònica	I.8	Fallada servei comunicacions				4					3,00					12,00		Assumir

		E.2	Erros d'administrador		2	2	2			0,25	2,25	3,00			0,50	4,50	6,00		Assumir
		E.15	Alteració accidental de la informació			3		3			1,50		0,80			4,50		2,40	Assumir
		E.18	Destrucció de la informació				2	2				3,00	0,80				6,00	1,60	Assumir
		E.19	Fuga de informació		5					0,25					1,25				Assumir
		E.23	Errors manteniment o actualització d'equips				2					3,00					6,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				2					3,00					6,00		Assumir
		A.5	Suplantació d'identitat	3	3	3			2,00	2,50	0,60			6,00	7,50	1,80			Assumir
		A.6	Abús de privilegis d'accés		3	3	3			0,25	0,60	0,60			0,75	1,80	1,80		Assumir
		A.7	Ús no previst		5	5	5			0,25	0,60	0,60			1,25	3,00	3,00		Assumir
		A.11	Accés no autoritzat		3	3				0,25	0,60				0,75	1,80			Assumir
		A.15	Modificació deliberada de la informació			2					2,25					4,50			Assumir
		A.19	Divulgació de informació		3					0,25					0,75				Assumir
		A.24	Denegació de servei				2					3,00					6,00		Assumir

Taula 22. Risc comunicacions

ID. Actiu	Actiu	ID. Amenaça	Amenaça	Probabilitat					Impacte					RISC					Acció
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
S.1	Directori Actiu	E.1	Errors d'usuaris		5	5	5			0,45	0,40	0,50			2,25	2,00	2,50		Assumir
		E.2	Erros d'administrador		3	3	3			0,45	0,45	5,00			1,35	1,35	15,00		Assumir
		E.15	Alteració accidental de la informació			3		3			4,00		1,80			12,00		5,40	Assumir
		E.18	Destrucció de la informació				2	2				5,00	1,80				10,00	3,60	Assumir
		E.19	Fuga de informació		2					0,45					0,90				Assumir
		E.23	Errors manteniment o actualització d'equips				3					2,00					6,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				3					5,00					15,00		Assumir
		A.5	Suplantació d'identitat	3	3	3			1,80	1,80	0,40			5,40	5,40	1,20			Assumir
		A.6	Abús de privilegis d'accés		3	3	3			0,45	0,40	0,50			1,35	1,20	1,50		Assumir
		A.7	Ús no previst		2	2	2			0,45	0,40	0,50			0,90	0,80	1,00		Assumir
		A.11	Accés no autoritzat		2	2				1,80	0,40				3,60	0,80			Assumir
		A.15	Modificació deliberada de la informació			3					4,00					12,00			Assumir
		A.18	Destrucció de la informació				2	2				5,00	1,80				10,00	3,60	Assumir
		A.19	Divulgació de informació		2					0,45					0,90				Assumir
		A.24	Denegació de servei				2					5,00					10,00		Assumir
S.2	Web	E.1	Errors d'usuaris		5	5	5			0,15	0,40	0,35			0,75	2,00	1,75		Assumir
		E.2	Erros d'administrador		3	3	3			1,50	0,45	5,25			4,50	1,35	**15,75**		**Reduir**

		E.15	Alteració accidental de la informació			4		4			4,00		1,20			**16,00**		4,80	**Reduir**
		E.18	Destrucció de la informació				3	3				5,25	1,20				**15,75**	3,60	**Reduir**
		E.19	Fuga de informació		3					0,60					1,80				Assumir
		E.23	Errors manteniment o actualització d'equips				2					5,25					10,50		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				2					7,00					14,00		Assumir
		A.5	Suplantació d'identitat	3	3	3			1,20	0,60	1,60			3,60	1,80	4,80			Assumir
		A.6	Abús de privilegis d'accés		2	2	2			0,60	1,60	1,40			1,20	3,20	2,80		Assumir
		A.7	Ús no previst		3	3	3			0,60	1,60	1,40			1,80	4,80	4,20		Assumir
		A.11	Accés no autoritzat		3	3				1,50	1,60				4,50	4,80			Assumir
		A.15	Modificació deliberada de la informació			3					4,00					12,00			Assumir
		A.18	Destrucció de la informació				2	2				5,25	1,20				10,50	2,40	Assumir
		A.19	Divulgació de informació		2					0,60					1,20				Assumir
		A.24	Denegació de servei				2					7,00					14,00		Assumir
S.3	Serveis al usuari final	E.1	Errors d'usuaris		4	4	4			10,00	4,00	2,00			**40,00**	**16,00**	8,00		**Reduir**
		E.2	Erros d'administrador		2	2	2			2,00	0,45	2,00			4,00	0,90	4,00		Assumir
		E.15	Alteració accidental de la informació			3		3			6,00		1,20			**18,00**		3,60	**Reduir**
		E.18	Destrucció de la informació				3	3				7,50	3,00				**22,50**	9,00	**Reduir**
		E.19	Fuga de informació		4					10,00					**40,00**				**Evitar**
		E.23	Errors manteniment o actualització d'equips				4					7,50					**30,00**		**Reduir**
		E.24	Caiguda de sistema per esgotament de recursos				3					7,50					**22,50**		**Reduir**
		A.5	Suplantació d'identitat	2	2	2			4,50	5,00	4,00			9,00	10,00	8,00			Assumir
		A.6	Abús de privilegis d'accés		2	2	2			2,00	1,60	2,00			4,00	3,20	4,00		Assumir
		A.7	Ús no previst		2	2	2			10,00	1,60	2,00			**20,00**	3,20	4,00		**Evitar**
		A.11	Accés no autoritzat		2	2				10,00	1,60				**20,00**	3,20			**Evitar**
		A.15	Modificació deliberada de la informació			2					6,00					12,00			Assumir
		A.18	Destrucció de la informació				2	2				7,50	1,20				15,00	2,40	Assumir
		A.19	Divulgació de informació		2					10,00					**20,00**				**Reduir**
		A.24	Denegació de servei				2					10,00					**20,00**		**Reduir**
S.4	VPN	E.1	Errors d'usuaris		4	4	4			0,25	0,25	0,10			1,00	1,00	0,40		Assumir
		E.2	Erros d'administrador		2	2	2			1,00	0,45	2,00			2,00	0,90	4,00		Assumir
		E.15	Alteració accidental de la informació			3		3			1,00		1,20			3,00		3,60	Assumir
		E.18	Destrucció de la informació				3	3				1,50	1,20				4,50	3,60	Assumir
		E.19	Fuga de informació		2					3,75					7,50				Assumir
		E.23	Errors manteniment o actualització d'equips				2					2,00					4,00		Assumir

		E.24	Caiguda de sistema per esgotament de recursos				4					1,50						6,00		Assumir
		A.5	Suplantació d'identitat	3	3	3			4,50	3,75	0,25			13,50	11,25	0,75			Assumir
		A.6	Abús de privilegis d'accés		3	3	3			1,00	1,00	0,40			3,00	3,00	1,20		Assumir
		A.7	Ús no previst		3	3	3			1,00	1,00	0,40			3,00	3,00	1,20		Assumir
		A.11	Accés no autoritzat		3	3				5,00	1,00				15,00	3,00			Assumir
		A.15	Modificació deliberada de la informació			3					2,50					7,50			Assumir
		A.18	Destrucció de la informació				2	2				1,50	3,00				3,00	6,00	Assumir
		A.19	Divulgació de informació		3					5,00					15,00				Assumir
		A.24	Denegació de servei				3					2,00					6,00		Assumir
S.5	Intranet	E.1	Errors d'usuaris		4	4	4			4,50	0,40	0,50			**18,00**	1,60	2,00		**Reduir**
		E.2	Erros d'administrador		2	2	2			4,50	0,45	5,00			9,00	0,90	10,00		Assumir
		E.15	Alteració accidental de la informació			3		3			4,00		1,80			12,00		5,40	Assumir
		E.18	Destrucció de la informació				3	3				10,00	1,80				**30,00**	5,40	**Reduir**
		E.19	Fuga de informació		4					9,00					**36,00**				**Evitar**
		E.23	Errors manteniment o actualització d'equips				2					7,50					15,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				2					7,50					15,00		Assumir
		A.5	Suplantació d'identitat	5	5	5			5,25	9,00	1,60			**26,25**	**45,00**	8,00			**Evitar**
		A.6	Abús de privilegis d'accés		3	3	3			1,80	1,60	0,50			5,40	4,80	1,50		Assumir
		A.7	Ús no previst		3	3	3			6,75	1,60	2,00			**20,25**	4,80	6,00		**Evitar**
		A.11	Accés no autoritzat		3	3				9,00	1,60				**27,00**	4,80			**Evitar**
		A.15	Modificació deliberada de la informació			3					6,00					**18,00**			**Reduir**
		A.18	Destrucció de la informació				3	3				5,00	4,50				15,00	13,50	Assumir
		A.19	Divulgació de informació		3					6,75					**20,25**				**Reduir**
		A.24	Denegació de servei				3					5,00					15,00		Assumir
S.6	O365 (correu i fitxers)	E.1	Errors d'usuaris		4	4	4			2,25	0,15	0,15			9,00	0,60	0,60		Assumir
		E.2	Erros d'administrador		2	2	2			0,60	0,45	2,25			1,20	0,90	4,50		Assumir
		E.15	Alteració accidental de la informació			3		3			0,60		0,15			1,80		0,45	Assumir
		E.18	Destrucció de la informació				3	3				1,50	1,50				4,50	4,50	Assumir
		E.19	Fuga de informació		4					3,00					12,00				Assumir
		E.23	Errors manteniment o actualització d'equips				2					1,50					3,00		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				2					3,00					6,00		Assumir
		A.5	Suplantació d'identitat	3	3	3			3,00	3,00	0,60			9,00	9,00	1,80			Assumir
		A.6	Abús de privilegis d'accés		3	3	3			0,60	0,15	0,15			1,80	0,45	0,45		Assumir
		A.7	Ús no previst		3	3	3			0,60	0,15	0,15			1,80	0,45	0,45		Assumir

		A.11	Accés no autoritzat		3	3				2,25	0,60				6,75	1,80			Assumir
		A.15	Modificació deliberada de la informació			3					0,60					1,80			Assumir
		A.18	Destrucció de la informació				3	3				1,50	0,60				4,50	1,80	Assumir
		A.19	Divulgació de informació		3					3,00					9,00				Assumir
		A.24	Denegació de servei				3					3,00					9,00		Assumir
S.7	Emmagatzematge de dades local	E.1	Errors d'usuaris		4	4	4			0,60	0,60	1,50			2,40	2,40	6,00		Assumir
		E.2	Erros d'administrador		2	2	2			2,25	0,45	2,25			4,50	0,90	4,50		Assumir
		E.15	Alteració accidental de la informació			4		4			2,25		0,60			9,00		2,40	Assumir
		E.18	Destrucció de la informació				3	3				2,25	0,60				6,75	1,80	Assumir
		E.19	Fuga de informació		3					3,00					9,00				Assumir
		E.23	Errors manteniment o actualització d'equips				2					2,25					4,50		Assumir
		E.24	Caiguda de sistema per esgotament de recursos				2					3,00					6,00		Assumir
		A.5	Suplantació d'identitat	3	3	3			3,00	3,00	0,60			9,00	9,00	1,80			Assumir
		A.6	Abús de privilegis d'accés		3	3	3			0,60	0,60	0,60			1,80	1,80	1,80		Assumir
		A.7	Ús no previst		5	5	5			0,60	0,60	0,60			3,00	3,00	3,00		Assumir
		A.11	Accés no autoritzat		3	3				3,00	0,60				9,00	1,80			Assumir
		A.15	Modificació deliberada de la informació			3					2,25					6,75			Assumir
		A.18	Destrucció de la informació				3	3				2,25	0,60				6,75	1,80	Assumir
		A.19	Divulgació de informació		3					3,00					9,00				Assumir
		A.24	Denegació de servei				3					3,00					9,00		Assumir

Taula 23. Risc serveis

ID. Actiu	Actiu	ID. Amenaça	Amenaça	Probabilitat					Impacte					RISC					Acció
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
MED.1	Cabina de discs (emmagatzematge de xarxa)	N.1	Foc				1					9,00					9,00		Assumir
		N.2	Danys per aigua				1					9,00					9,00		Assumir
		N.9	Origen meteorològic				1					9,00					9,00		Assumir
		I.5	Averia d'origen físic o lògic				1					9,00					9,00		Assumir
		I.6	Tall elèctric				1					9,00					9,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					9,00					9,00		Assumir
		I.10	Degradació dels suports d'emmagatzematge				2					6,75					13,50		Assumir
		E.1	Errors d'usuaris		5	5	5			2,00	1,80	0,45			10,00	9,00	2,25		Assumir
		E.2	Erros d'administrador		3	3	3			5,00	1,80	4,50			15,00	5,40	13,50		Assumir
		E.15	Alteració accidental de la informació			3		3			6,75		2,00			**20,25**		6,00	**Reduir**

		E.18	Destrucció de la informació				2	2				6,75	2,00				13,50	4,00	Assumir
		E.19	Fuga de informació		1					10,00					10,00				Assumir
		E.25	Pèrdua d'equips		1		1			2,00		9,00			2,00		9,00		Assumir
		A.7	Ús no previst		4	4	4			2,00	0,45	0,45			8,00	1,80	1,80		Assumir
		A.11	Accés no autoritzat		4	4				7,50	1,80				**30,00**	7,20			**Evitar**
		A.15	Modificació deliberada de la informació			3					9,00					**27,00**			**Reduir**
		A.18	Destrucció de la informació				2	2				9,00	2,00				**18,00**	4,00	**Reduir**
		A.19	Divulgació de informació		2					2,00					4,00				Assumir
		A.25	Robatori		1		1			7,50		9,00			7,50		9,00		Assumir

Taula 24. Risc suports d'informació

ID. Actiu	Actiu	ID. Amenaça	Amenaça	Probabilitat					Impacte					RISC					Acció
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
AUX.1	Climatització CPD's	N.1	Foc				1					10,00					10,00		Assumir
		N.2	Danys per aigua				1					7,50					7,50		Assumir
		N.9	Origen meteorològic				1					7,50					7,50		Assumir
		I.5	Averia d'origen físic o lògic				2					7,50					15,00		Assumir
		I.6	Tall elèctric				2					7,50					15,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				2					7,50					15,00		Assumir
		I.9	Interrupció d'altres serveis				2					2,00					4,00		Assumir
		E.25	Pèrdua d'equips		1		1			0,05		5,00			0,05		5,00		Assumir
		A.7	Ús no previst		1	1	1			0,05	4,50	0,50			0,05	4,50	0,50		Assumir
		A.11	Accés no autoritzat		1	1				0,05	0,45				0,05	0,45			Assumir
		A.25	Robatori		1		1			0,05		5,00			0,05		5,00		Assumir
AUX.2	Control de portes	N.1	Foc				1					6,00					6,00		Assumir
		N.2	Danys per aigua				1					1,20					1,20		Assumir
		N.9	Origen meteorològic				1					1,20					1,20		Assumir
		I.5	Averia d'origen físic o lògic				2					3,00					6,00		Assumir
		I.6	Tall elèctric				2					0,30					0,60		Assumir
		I.7	Condicions inadequades Temperatura o humitat				2					0,30					0,60		Assumir
		I.9	Interrupció d'altres serveis				2					0,30					0,60		Assumir
		E.25	Pèrdua d'equips		1		1			0,40		1,20			0,40		1,20		Assumir
		A.7	Ús no previst		1	1	1			0,40	0,35	0,30			0,40	0,35	0,30		Assumir
		A.11	Accés no autoritzat		1	1				6,00	0,35				6,00	0,35			Assumir

		A.25	Robatori		1		1			4,00		1,20			4,00		1,20		Assumir
AUX.3	Càmeres Seguretat	N.1	Foc				1					3,00					3,00		Assumir
		N.2	Danys per aigua				2					1,50					3,00		Assumir
		N.9	Origen meteorològic				2					1,50					3,00		Assumir
		I.5	Averia d'origen físic o lògic				3					0,60					1,80		Assumir
		I.6	Tall elèctric				3					0,60					1,80		Assumir
		I.7	Condicions inadequades Temperatura o humitat				2					0,15					0,30		Assumir
		I.9	Interrupció d'altres serveis				2					0,15					0,30		Assumir
		E.25	Pèrdua d'equips		2		2			0,30		0,60			0,60		1,20		Assumir
		A.7	Ús no previst		3	3	3			4,50	0,30	0,60			13,50	0,90	1,80		Assumir
		A.11	Accés no autoritzat		3	3				4,50	0,30				13,50	0,90			Assumir
		A.25	Robatori		3		3			0,30		3,00			0,90		9,00		Assumir
AUX.4	SAI 's	N.1	Foc				1					10,00					10,00		Assumir
		N.2	Danys per aigua				1					5,00					5,00		Assumir
		N.9	Origen meteorològic				1					5,00					5,00		Assumir
		I.5	Averia d'origen físic o lògic				2					5,00					10,00		Assumir
		I.6	Tall elèctric				2					2,00					4,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				2					2,00					4,00		Assumir
		I.9	Interrupció d'altres serveis				2					0,50					1,00		Assumir
		E.25	Pèrdua d'equips		1		1			0,05		5,00			0,05		5,00		Assumir
		A.7	Ús no previst		1	1	1			0,05	2,00	2,00			0,05	2,00	2,00		Assumir
		A.11	Accés no autoritzat		1	1				0,05	0,50				0,05	0,50			Assumir
		A.25	Robatori		1		1			0,05		5,00			0,05		5,00		Assumir
AUX.5	Grup electrogen	N.1	Foc				1					9,00					9,00		Assumir
		N.2	Danys per aigua				1					9,00					9,00		Assumir
		N.9	Origen meteorològic				1					6,75					6,75		Assumir
		I.5	Averia d'origen físic o lògic				2					6,75					13,50		Assumir
		I.6	Tall elèctric				2					0,45					0,90		Assumir
		I.7	Condicions inadequades Temperatura o humitat				2					1,80					3,60		Assumir
		I.9	Interrupció d'altres serveis				2					4,50					9,00		Assumir
		E.25	Pèrdua d'equips		1		1			0,05		9,00			0,05		9,00		Assumir
		A.7	Ús no previst		1	1	1			0,05	0,40	0,45			0,05	0,40	0,45		Assumir
		A.11	Accés no autoritzat		1	1				0,05	0,40				0,05	0,40			Assumir
		A.25	Robatori		1		1			0,05		9,00			0,05		9,00		Assumir

AUX.6	Robot de cintes	N.1	Foc				1					10,00					10,00		Assumir
		N.2	Danys per aigua				1					10,00					10,00		Assumir
		N.9	Origen meteorològic				1					10,00					10,00		Assumir
		I.5	Averia d'origen físic o lògic				1					10,00					10,00		Assumir
		I.6	Tall elèctric				1					10,00					10,00		Assumir
		I.7	Condicions inadequades Temperatura o humitat				1					10,00					10,00		Assumir
		I.9	Interrupció d'altres serveis				1					0,50					0,50		Assumir
		E.25	Pèrdua d'equips		1		1			1,80		10,00			1,80		10,00		Assumir
		A.7	Ús no previst		2	2	2			0,45	0,50	0,50			0,90	1,00	1,00		Assumir
		A.11	Accés no autoritzat		2	2				1,80	0,50				3,60	1,00			Assumir
		A.25	Robatori		1		1			4,50		10,00			4,50		10,00		Assumir
AUX.7	Mobiliari oficina	N.1	Foc				1					8,00					8,00		Assumir
		N.2	Danys per aigua				2					6,00					12,00		Assumir
		N.9	Origen meteorològic				2					1,60					3,20		Assumir
		I.5	Averia d'origen físic o lògic				3					1,60					4,80		Assumir
		I.6	Tall elèctric				1					0,40					0,40		Assumir
		I.7	Condicions inadequades Temperatura o humitat				3					0,40					1,20		Assumir
		I.9	Interrupció d'altres serveis				1					0,40					0,40		Assumir
		E.25	Pèrdua d'equips		2		2			0,20		6,00			0,40		12,00		Assumir
		A.7	Ús no previst		3	3	3			0,05	0,80	0,40			0,15	2,40	1,20		Assumir
		A.11	Accés no autoritzat		3	3				0,50	0,20				1,50	0,60			Assumir
		A.25	Robatori		2		2			0,05		6,00			0,10		12,00		Assumir

Taula 25. Risc equipament auxiliar

ID. Actiu	Actiu	ID. Amenaça	Amenaça	Probabilitat					Impacte					RISC					Acció
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	
P.1	Administradors	E.7	Deficiències amb la organització				3					3,00					9,00		Assumir
		E.19	Fuga de informació		2					7,50					15,00				Assumir
		E.28	Indisponiblitat del personal				3					3,00					9,00		Assumir
		A.28	Indisponiblitat del personal				3					3,00					9,00		Assumir
		A.29	Extorsió	2	2		2		4,50	7,50		0,30		9,00	15,00		0,60		Assumir
		A.30	Enginyeria social	2	2		2		4,50	7,50		0,30		9,00	15,00		0,60		Assumir
P.2	Programadors	E.7	Deficiències amb la organització				4					1,50					6,00		Assumir
		E.19	Fuga de informació		2					7,50					15,00				Assumir

		E.28	Indisponiblitat del personal				3					1,50					4,50		Assumir
		A.28	Indisponiblitat del personal				3					1,50					4,50		Assumir
		A.29	Extorsió	2	2		2		4,50	7,50		0,15		9,00	15,00		0,30		Assumir
		A.30	Enginyeria social	2	2		2		3,00	5,00		0,15		6,00	10,00		0,30		Assumir
P.3	Treballadors	E.7	Deficiències amb la organització				4					0,60					2,40		Assumir
		E.19	Fuga de informació		4					10,00					**40,00**				**Evitar**
		E.28	Indisponiblitat del personal				4					0,60					2,40		Assumir
		A.28	Indisponiblitat del personal				4					0,60					2,40		Assumir
		A.29	Extorsió	1	1		1		3,00	7,50		0,15		3,00	7,50		0,15		Assumir
		A.30	Enginyeria social	3	3		3		4,50	10,00		0,15		13,50	**30,00**		0,45		**Reduir**
P.4	Voluntaris	E.7	Deficiències amb la organització				4					0,15					0,60		Assumir
		E.19	Fuga de informació		4					10,00					**40,00**				**Evitar**
		E.28	Indisponiblitat del personal				4					0,15					0,60		Assumir
		A.28	Indisponiblitat del personal				4					0,15					0,60		Assumir
		A.29	Extorsió	1	1		1		3,00	7,50		0,15		3,00	7,50		0,15		Assumir
		A.30	Enginyeria social	3	3		3		4,50	10,00		0,15		13,50	**30,00**		0,45		**Reduir**
P.5	Proveïdors	E.7	Deficiències amb la organització				4					1,60					6,40		Assumir
		E.19	Fuga de informació		2					7,50					15,00				Assumir
		E.28	Indisponiblitat del personal				2					0,40					0,80		Assumir

Taula 26. Risc personal

Analitzant les dades obtingudes veiem que l'organització ha de tenir en compte els següents riscos i procedir al seu tractament. Així que tindrem 4 possibles estats R (Reduir), E (Evitar), D (Delegar) i finalment Assumir.

Origen	ID. A	Actius																										
		L.1	L.2	L.3	HW.10	HW.14	SW.1	SW.2	SW.4	D.1	D.2	D.3	D.4	D.5	D.6	D.7	COM.1	COM.3	S.2	S.3	S.5	S.6	S.7	MED.1	P.3	P.4
Origen Natural	*N.2*				R																					
Origen Industrial	*I.5*				R		R	R	D																	
	I.8																R	R								
Errors i fallades no intencionades	*E.1*									R	R	R	R	R						R	R					
	E.2											R			R	R	R	R	R					R		
	E.8						R	R	D																	
	E.15											R				R			R	R						
	E.18						R	R	D	R	R	R				R	R	R	R	R	R					
	E.19						E	E	D	E	E	E	E				E	E		E	E				E	E
	E.20								D																	
	E.21								D																	
	E.23																R	R		R						
	E.24					R											R	R		R						
	E.25				R																					
Atacs Intencionats	*A.4*									R	R	R	R			R										
	A.5						E	E	D	E	E	E	E		E		E	E			E					
	A.7		E		R													E		E	E					
	A.8						R	R																		
	A.11	E	E	E	R		E	E		E	E	E	E		E		E	E		E	E			E		
	A.15						R	R	D	R	R	R	R		R						R			R		
	A.18						R	R	D	R	R	R				R								R		
	A.19						R	R		R	R	R	R		R			R		R	R					
	A.24																R	R		R						
	A.25				R																					
	A.30																								R	R

Taula 27. Riscs destacables

Com podem observar la major part de incidents són degut a errors de usuaris o per accions "malintencionades" o conscients, ja sigui per falta de conscienciació o de formació.

5. Pla de Projectes

Un cop avaluat el risc i coneixent el nivell de maduresa actual del sistema de l'organització es l'hora de definir els projectes per tal de donar compliment a la ISO27001 i millorar el sistema i obtenir el nivell de maduresa desitjat.

Cada proposta de projectes ha d'incloure una sèrie d'elements com són:

- Nom del projecte i identificació.
- Descripció i objectius on es descriu quina és la motivació i l'objectiu del projecte.
- Controls i dominis de la ISO que quedaran millorats amb la realització del projecte.
- Amenaces a tractar amb la implementació del projecte detectades a l'anàlisi de risc.
- Prioritat i Planificació on s'indicarà el nivell de prioritat i la durada del projecte (curt, mig i llarg termini).
- Cost i nivell de millora en indica quin cost suposa per l'organització i quina millora implica en el nivell de maduresa.
- Responsable ens indica qui es el responsable de la realització del projecte.

En aquest punt cal definir una sèrie de condicions, com poden ser els costos de preu per hora dels tècnics especialistes, mitja de Treballador i directius.

Cost directiu – 45€/h
Cost tècnic especialista – 30€/h
Cost mig treballador – 20€/h

Indicarem també la quantitat de personal de cada Grup que implica i les hores dedicades per cadascun dels treballadors.

El càlcul del ROI (*Return On Investment*), retorn de la inversió, és un aspecte important en els projectes i es fa de la següent manera.

$$ROI = \frac{(Guany\ de\ la\ inversió - Cost\ de\ la\ inversió)}{Cost\ de\ la\ inversió} \times 100$$

Cal dir, que en el cas dels projectes sobre ciberseguretat i formació la quantificació econòmica del ROI és una qüestió molt hipotètica i per tant no entrarem a fer un supòsit econòmic concret, ja que per exemple en qüestions com la implementació d'un antivirus té que veure amb els incidents evitats, on s'eviten i quin hauria pogut ser la repercussió, i com que és una cosa completament hipotètica preferim no fer un anàlisi d'aquest tipus. No obstant si que indicarem si aquest ROI és Molt Alt, Alt, Mig o Baix.

Projecte 1. Campanya de conscienciació sobre la seguretat en els sistemes d'informació a l'organització

Nom	**ID**	Campanya de conscienciació sobre la seguretat en els sistemes d'informació a l'organització		Proj01
Objectiu		Millorar els coneixements, les habilitats i la conscienciació del personal en l'àmbit de la seguretat dels sistemes d'informació i les bones practiques		
Controls de la ISO		A.7.2.2. Conscienciació, educació i capacitació en seguretat de la informació A.9.3 Responsabilitat de l' usuari		
Dominis de la ISO		A.7.3 Conscienciació A.7.4 Comunicació		
Amenaces a tractar		E.1 Errors d'usuari. E.8 Difusió de software maligne. E.15 Alteració accidental de la informació E.18 Destrucció de la informació E.19 Fuga de informació E.20 Vulnerabilitat dels programes E.24 Caiguda de sistema per esgotament de recursos E.25 Pèrdua d'equips A.5 Suplantació d'identitat A.6 Abús de privilegis d'accés A.7 Us no previst A.8 Difusió de software maligne A.11 Accés no autoritzat		
Prioritat	**Planificació**	Alta	Periòdica – llarg termini	
Cost	**Millora**	31710€		L3 – L4
Responsable		CIO, RSI, directors de departament		

Taula 28. Projecte 1 Campanya de conscienciació

Degut al gran número d'incidents detectats, tant voluntaris com involuntaris, per part dels treballadors i voluntaris és important la realització d'aquests campanyes de conscienciació. Juntament amb les guies i procediments desenvolupats pel departament de SI destinats als usuaris es podria assolir un nivell de maduresa gestionat i mesurable.

La responsabilitat recau en tots els directors de departament de l'organització i en el responsable de seguretat, ja que han de procurà que els treballadors i voluntaris segueixin les directrius corresponents i de fer difusió d'aquestes campanyes.

El cost del projecte el trobem desglossat de la següent manera:

Personal	Nº	Fase	hores	Cost	Total
CIO	1	Creació grup de treball i definició de campanyes	2	45€	90€
RSI	1		4	45€	180€
Tècnic	2		2	30€	120€
Tècnic	2	Desenvolupament de les campanyes	16	30€	960€
CIO	1	Revisió i aprovació de les campanyes	1	45€	45€
RSI	1		1	45€	45€
Tècnic	2		1	30€	60€

Directius	2		1	45€	90€
Tècnic	1	Programació llançament de campanyes	4	30€	120€
Treballadors	15000	Hores de conscienciació	0,1	20€	30000€
				Total	**31710€**

Taula 29. Resum d'hores destinades al Proj01

ROI - ↑↑↑ Molt Alt

Les campanyes de conscienciació són difícils de quantificar-li un valor econòmic, una repercussió directa és complicada, però l'organització està convençuda que el ROI és molt alt, ja que qualsevol incident de seguretat pot arribar a tenir unes repercussions econòmiques molt altes per l'organització.

L'eficiència d'aquestes campanyes es veurà amb el temps amb la disminució de incidents de seguretat detectats en comparació amb els detectats abans de les campanyes llençades.

Projecte 2. Formacions sobre l'ús de les eines informàtiques comuns a l'organització.

Nom	**ID**	Formacions internes d'ús de les eines informàtiques comuns a l'organització	Proj02
Objectiu		Millorar els coneixements, les habilitats i la competència en l'ús de les eines informàtiques que són d'ús comú a l'organització per tal de minimitzar els errors en l'ús de les mateixes.	
Controls de la ISO		A.7.2.2. Conscienciació, educació i capacitació en seguretat de la informació A.9.3 Responsabilitat de l' usuari	
Dominis de la ISO		A.7.2 Competència A.7.4 Comunicació	
Amenaces a tractar		E.1 Errors d'usuari. E.8 Difusió de software maligne. E.15 Alteració accidental de la informació E.18 Destrucció de la informació E.19 Fuga de informació E.20 Vulnerabilitat dels programes E.24 Caiguda de sistema per esgotament de recursos E.25 Pèrdua d'equips A.5 Suplantació d'identitat A.6 Abús de privilegis d'accés A.7 Us no previst A.8 Difusió de software maligne A.11 Accés no autoritzat	
Prioritat	**Planificació**	Alta	Periòdica – llarg termini
Cost	**Millora**	163910€	L3 – L4
Responsable		CIO, Responsable SI i directors de departament	

Taula 30. Projecte 2 Cursos de Formació interna

S'ha detectat un nivell baix en l'ús de les eines informàtiques pròpies de l'organització, per part dels treballadors i voluntaris. Aquest nivell pot ser degut tant a l'alt nivell de rotació en alguns departaments, com en la falta d'un programa

específic de formació continuada a nous treballadors i millora de les competències en els treballadors actuals.

A part de les eines pròpies, també es realitzaran cursos per augmentar les competències en eines d'ús comú, com són les eines ofimàtiques i cursos de bones pràctiques. És important la realització d'aquests cursos que juntament amb les guies i procediments desenvolupats pel departament de TID destinats als usuaris es podria assolir un nivell de maduresa gestionat i mesurable.

La responsabilitat recau en tots els directors de departament de l'organització, ja que han de procurà que els treballadors i voluntaris segueixin un procediment de formació constant i continuada per part de treballadors i voluntaris de l'organització.

El cost del projecte el trobem desglossat de la següent manera:

Personal	Nº	Fase	hores	Cost	Total
CIO	1	Creació grup de treball i definició de cursos	2	45€	90€
RSI	1		4	45€	180€
Tècnic	10		2	30€	600€
Tècnic	10	Preparació dels cursos	16	30€	4800€
Tècnic	1	Realització de cursos dos dies per setmana durant 4 hores	368	30€	11040€
Treballadors	20		368	20€	147200€
				Total	**163910€**

Taula 31. Resum d'hores destinades al Proj02

ROI - ↑↑ Molt Alt

El ROI en projectes de formació no es pot fer d'una manera convencional, ja que en moltes ocasions no es pot repercutir a un valor econòmic. No obstant es pot tenir en compte el valor que aporten tant al propi treballador com a l'organització, es pot valorar si els cursos han millorar les habilitats dels treballadors, el grau de satisfacció d'aquests amb els cursos.

Projecte 3. Formació i cursos especialitzats per Administradors de sistema

Nom	**ID**	Formació i cursos especialitzats per Administradors de sistema	Proj03
Objectiu		Realitzar formacions especifiques en diferents àmbits per millorar les capacitats dels administradors i minimitzar així errors en la seves tasques habituals.	
Controls de la ISO		A.6.1 Organització interna A.12 Seguretat de les Operacions A.13 Seguretat de les Comunicacions A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació	
Amenaces a tractar		E.2 Errors d'administrador	
Prioritat	**Planificació**	Mitja	Periòdica – llarg termini
Cost	**Millora**	126540€	L3 – L4
Responsable		CIO, RSI, responsable SI, Director de RH	

Taula 32. Projecte 3 Cursos de Formació específica a administradors

Un dels punts dèbils de l'àrea de SI és l'estancació de la formació dels administradors sobretot en les seus territorials. Per tant per minimitzar errors relacionats amb l'administració cal formar al personal en aspectes concrets. Per això cal destinar una partida pressupostaria a la formació d'aquest personal segons les necessitats vigents del moment.

La formació ha de ser periòdica i constant i específica per les tasques que realitzi cada administrador. Aquesta actuació tot i ser necessària no es prioritària, ja que els administradors ja estan capacitats per les feines que realitzen.

El cost del projecte el trobem desglossat de la següent manera:

Personal	Nº	Fase	hores	Cost	Total
CIO	1	Anàlisi de necessitats	3	45€	135€
RSI	1		3	45€	135€
Resp. SI	1		3	45€	135€
Direc. RH	1		3	45€	135€
Tècnic	45	Realització dels cursos	60	30€	81000€
				Cost dels cursos	45000€
				Total	**126540€**

Taula 33. Resum d'hores destinades al Proj03

ROI - ↑↑ Molt Alt

La realització de cursos especialitzats per a administradors, a part de la pròpia formació de la que ja disposen, té un ROI elevat, ja que tenir personal format evitarà haver de contractar personal extra format amb un cost elevat o internalitzar algunes de les funcions que no es podrien fer per falta de formació.

Projecte 4. Implantació d'un nou sistema antivirus de nova generació

Nom	**ID**	Implementació nou sistema antivirus de nova generació (Crowdstrike)		Proj04
Objectiu		Contractació d'una plataforma per la gestió del antivirus en els dispositius de l'organització		
Controls de la ISO		A.12.2 Protecció contra el programari maliciós (malware).		
Amenaces a tractar		I.5 Averia d'origen físic o lògic E.8 Difusió de software maligne E.18 Destrucció de la informació E.19 Fuga de informació E.20 Vulnerabilitat dels programes E.21 Errors manteniment o actualització de programes A.5 Suplantació d'identitat A.8 Difusió de software maligne A.11 Accés no autoritzat A.15 Modificació deliberada de la informació A.18 Destrucció de la informació A.19 Divulgació d'informació		
Prioritat	**Planificació**	Alta	Curt termini	
Cost	**Millora**	325250€		L5
Responsable		RSI		

Taula 34. Projecte 4 Implementació nou sistema antivirus

El cost del projecte el trobem desglossat de la següent manera:

Personal	Nº	Fase	hores	Cost	Total
RSI	1	Reunions amb proveïdor i pla de treball	10	45€	450€
Tècnic	2	Implementació nou sistema	30	30€	1800€
				Cost plataforma	323000€
				Total	**325250€**

Taula 35. Resum d'hores destinades al Proj04

ROI - ↑ Alt

Ja es disposava d'un sistema antivirus tradicional i de prestigi, però l'evolució de les amenaces i dels atacs han portat a la decisió d'invertir en una nova plataforma d'antivirus de nova generació que ens permetran reduir l'impacte de les amenaces i millorar el rendiment dels equips.

Projecte 5. Revisió i millora del sistema de copies de seguretat

Nom	**ID**	Revisió i millora del sistema de copies de seguretat		Proj05
Objectiu		Millorar el sistema actual de copies de seguretat, fent una revisió tant del contingut de la informació a copiar, com dels medis i sistemes de rotació de cintes magnètiques. També cal revisar el sistema de custòdia de cintes.		
Controls de la ISO		A.12.3 Còpies de seguretat de la informació A.12.4.2 Protecció de la informació del registre A.14.3 Dades de prova		
Amenaces a tractar		E.1 Errors d'usuari E.15 Alteració accidental de la informació E.18 Destrucció de la informació A.15 Modificació deliberada de la informació A.18 Destrucció de la informació		
Prioritat	**Planificació**	Mitja	Curt termini	
Cost	**Millora**	1800€		L4
Responsable		CIO, responsable SI		

Taula 36. Projecte 5 Revisió i millora del sistema de copies de seguretat

L'organització actualment disposa dels recursos de Hardware suficients per la realització de les copies de seguretat. No obstant, el procediment existent de copies de seguretat és ja una mica antic i cal actualitzar-lo adaptant-lo tant al volum de dades actual, com al contingut. La migració de moltes dades al núvol de l'O365 fa que part de les copies de seguretat de les cabines de dades existents ja no siguin necessàries. Cal incloure al sistema de copies de seguretat existent la plataforma de desenvolupament de software i les dades de prova.

Aquest procediment cal revisar-lo però no és prioritari, ja que existeix un sistema de copies de seguretat que està ben definit, però com hem comentat és millorable.

Aquest projecte no implica un gran cost, tant sols les hores del personal destinades a la planificació i reprogramació.

Personal	Nº	Fase	hores	Cost	Total
Tècnic	2	Revisió i millora del sistema de copies de seguretat	30	30€	1800€
				Total	**1800€**

Taula 37. Resum d'hores destinades al Proj05

ROI - ↑↑ Molt Alt

Millorar els procediments de copies de seguretat i revisar cada poc temps les dades que s'han de copiar i les polítiques de rotació i manteniment no té una repercussió econòmica directa, no obstant la pèrdua de informació pot tenir repercussions econòmiques altes, ja sigui per hores de repetició de tasques realitzades o per pèrdua sensible de informació. Per tant creiem que el ROI és molt alt.

Projecte 6. Revisió i millores del control d'accessos a àrees segures

Nom	**ID**	Revisió i millores del control d'accessos a àrees segures		Proj06
Objectiu		Millorar el control d'accés a àrees restringides o sensibles que continguin informació o sistemes vitals per l'organització.		
Controls de la ISO		A.9 Control d'accés A.11 Seguretat física i de l'entorn		
Amenaces a tractar		A.7 Ús no previst A.11 Accés no autoritzat		
Prioritat	**Planificació**	Mitja	Curt termini	
Cost	**Millora**	3700€		L4
Responsable		CIO, RSI, responsable SI		

Taula 38. Projecte 6 Revisió i millora del control d'accessos a àrees segures

Cal ser mes estricte en el control d'accés a àrees segures, tant amb l'assignació de l'accés com en el manteniment. Cal procedimentar unes revisions periòdiques de revisió dels accessos. També cal posar sistemes de tancament automàtic en algunes portes d'accés d'aquestes àrees.

Personal	Nº	Fase	hores	Cost	Total
Tècnic	2	Revisió i millores del control d'accessos a àrees segures	50	30€	3000€
				Material	700€
				Total	**3700€**

Taula 39. Resum d'hores destinades al Proj06

ROI - ↓ Baix

Tot i que s'havien detectat deficiències amb el control d'accessos a àrees segures, és cert, que mai s'havia detectat cap incident, tot i que el risc existia. Per tant per tenir una disminució dels riscos i donar compliment als controls de la ISO 27001 i la baixa inversió que suposa adaptar i revisar aquest procediment tot i que el ROI creiem que és baix, és necessari.

Projecte 7. Implementació d'un MDM per la telefonía mòbil

Nom	**ID**	Implementació d'un MDM per la telefonía mòbil		Proj07
Objectiu		Contractació d'una plataforma per la gestió dels dispositius de telefonía mòbil		
Controls de la ISO		A.6.2.1 Política de dispositius mòbils		
Amenaces a tractar		N.2 Danys per aigua I.5 Averia d'origen físic o lògic E.1 Errors d'usuari E.18 Destrucció de la informació E.19 Fuga d'informació E.25 Pèrdua d'equips A.7 Ús no previst A.8 Difusió de software maligne A.11 Accés no autoritzat A.19 Divulgació d'informació A.25 Robatori		
Prioritat	**Planificació**	Alta	Mig termini	
Cost	**Millora**	1474620€		L5
Responsable		CIO, RSI		

Taula 40. Projecte 7 Implementació d'un MDM

La telefonía mòbil és un punt delicat en tota organització, ja que el control dels dispositius mòbils, la informació que contenen i la securització és un tema complicat. La implementació d'un MDM permetrà la gestió remota de tots els dispositius, controlar les aplicacions que es permeten i minimitzar els errors de configuració, també permet establir uns nivells de securització i configuracions estàndards.

Per realitzar aquest projecte, també caldrà la substitució de gran part del terminals mòbils de l'organització.

Personal	Nº	Fase	hores	Cost	Total
CIO	1	Reunió amb proveïdor i definició del projecte	5	45€	225€
RSI	1		5	45€	225€
RSI	1	Establiment equip tècnic	5	45€	225€
Tècnic	2		5	30€	300€
Tècnic	2	Formació	24	30€	1440€
Tècnic	2	Proves de Funcionament	30	30€	1800€
RSI	1	Revisió del registre de terminals amb inventari de terminals distribuïts	2	45€	90€
Resp. SI	1		2	45€	90€
Tècnics	10		30	30€	9000€
Resp. SI	1	Anàlisi de les necessitats de dispositius	5	45€	225€
Tècnic	10	Recepció dels nous terminals	40	30€	12000€
Tècnic	10	Distribució dels nous terminals	20	30€	6000€
Telèfons	14000	Cost per Terminal acordat		70€	1050000€
			Plataforma + formacions + assessorament		393000€
				Total	**1474620€**

Taula 41. Resum d'hores destinades al Proj06

ROI - ◄► Mig

Evitar incidents de seguretat, poder eliminar el contingut dels dispositius mòbils en cas de pèrdua o robatori, localitzar-los i poder establir una seguretat comuna a tots els dispositius mòbils ja justifica la inversió, es disminueix molt la quantitat de incidents de seguretat a notificar. A més a més es produeix una inversió en els dispositius mòbils i nous acords amb l'operador de telefonía, que s'haurien de realitzar, en algun moment, independentment de la implementació del MDM.

Projecte 8. Revisió i actualització dels procediments del departament de SI.

Nom	**ID**	Revisió i actualització dels procediments del departament de TID	Proj08
Objectiu		Cal revisar i actualitzar tots els procediments existents que són: • Normativa de protecció de Dades (Proj08_1) • Procediments de llocs de treball net i equip desatès (Proj08-2) • Ús dels equips (Proj08_3) • Ús del correu electrònic (Proj08_4) • Acords de confidencialitat (Proj08_5) • Guies d'orientació sobre missatgeria i xarxes socials (Proj08_6) • Guies de protecció de dades (Proj08_7) • Procediment exercici de dret (Proj08_8) • Notificació de bretxes de seguretat (Proj08_9) • Procediment de Teletreball (Proj08_10) • Guia de bones pràctiques (Proj08_11) • Procediments d'intercanvi d'informació (Proj08_12) • Procediment de desenvolupament segur (Proj08_13) • Pla de contingència, pla de proves, seguiment i millores (Proj08_14) • Guia d'administradors Territorials (Proj08_15) ○ Procediments Comunicació RH-TID alta, baixa, modificació d'usuaris ○ Procediment accés usuaris i gestió de claus ○ Procediments manteniment i actualització dels equips ○ Procediment d'instal·lació de programari • Procediment gestió de Logs (Proj08_16) • Procediments de contractació de proveïdors (Proj08_17) • Seguiment de incidents (Proj08_18) • Gestió de crisis (Proj08_19) • Llistats de procediments per serveis (Proj08_20)	

Controls de la ISO		A.5 Polítiques de la seguretat de la informació (Proj08) A.6.1.3 Contacte amb les autoritats (Proj08_9) A.6.2.2 Teletreball (Proj08_10) A.7 Seguretat relativa als recursos humans (Proj08_15) A.7.2 Durant l'ocupació (Proj08_8) A.8.1.3 Ús acceptable dels actius (Proj08_3) A.9 Control d'accés (Proj08_1, Proj08_2, Proj08_15) A.9.3 Responsabilitat de l'usuari (Proj08_6) A.10.1.1 Gestió de claus (Proj08_11) A.11.2 Seguretat dels equips (Proj08_2, Proj08_11, Proj08_15) A.12 Seguretat de les operacions (Proj08_15) A.12.1.4 Separació dels recursos de desenvolupament, prova i operació (Proj08_14) A.12.4 Registre i supervisió (Proj08_13, Proj08_14; Proj08_16) A.12.6 Gestió de les vulnerabilitats tècniques (Proj08_09) A.13.2 Intercanvi d'informació (Proj08_5, Proj08_12, Proj08_17) A.13.2.3 Missatgeria electrònica (Proj08_4, Proj08_6) A.14.2 Seguretat en el desenvolupament i en els processos de suport (Proj08_13, Proj08_15) A.15 Relació amb els proveïdors (Proj08_17) A.16.1 Gestió d'incidents de seguretat de la informació i millores (Proj08_8) A.18 Compliment (Proj08_7, Proj08_8)		
Dominis de la ISO		A.4 Context de l'organització A.5 Lideratge A.10 Millora		
Amenaces a tractar		[E] Errors i fallades no intencionades [A] Atacs intencionats		
Prioritat	**Planificació**	Alta	Curt termini	
Cost	**Millora**	38970€		L3 – L4
Responsable		CIO, RSI, responsable SI		

Taula 42. Projecte 8 Revisió procediments del departament de SI

En aquest projecte el que es pretén és revisar, actualitzar i adaptar tots els procediments existents a la normativa ISO 27001 i a les necessitats detectades en l'anàlisi del risc.

Personal	Nº	Fase	hores	Cost	Total
CIO	1	Assignació de projectes	4	45€	180€
DPO	1		4	45€	180€
RSI	1		4	45€	180€
Resp. SI	1		4	45€	180€
RSI	1	Revisió i actualització dels procediments	80	45€	3600€
DPO	1		80	45€	3600€
Resp. SI	1		80	45€	3600€
Tècnic	9		90	30€	24300€
Directius	1	Revisió i aprovació dels procediments redactats	10	45€	450€
CIO	1		20	45€	900€
DPO	1		20	45€	900€
RSI	1		20	45€	900€
				Total	**38970€**

Taula 43. Resum d'hores destinades al Proj08

ROI - ↓ Baix

Al igual que els projectes de formació, la revisió dels procediments existents per tal d'adaptar-los a la ISO 27001 no comporten una repercussió econòmica

directa. No obstant, aquests projectes son necessaris per el compliment de la ISO.

Projecte 9. Nous procediments SI

Nom	**ID**	Nous procediments del departament de SI	Proj09
Objectiu		Cal crear aquells procediments que manquen en la declaració d'aplicabilitat i els que comportin una millora en la reducció del risc de l'organització: • Revisió infraestructura de seu locals i pla de millores (Proj09_1) • Gestió de claus criptogràfiques (Proj09_2) • Pla de continuïtat de negoci (Proj09_3) • Procediment de contacte amb grups especials (Proj09_4) • Procediment gestió de projectes (Proj09_5) • Procediment per l'adquisició de nous components (Proj09_6)	
Controls de la ISO		A.5 Polítiques de la seguretat de la informació (Proj09) A.6.1.4 Contacte amb grups d' interès especial (Proj09_4) A.6.1.5 Seguretat de la informació en la gestió de projecte (Proj09_5) A.10.1.2 Gestió de claus (Proj09_2) A.11 Seguretat física i de l'entorn (Proj09_1) A.12 Seguretat de les operacions (Proj09_1, Proj09_5) A.14.1.1 Anàlisi de requisits i especificacions de seguretat de la informació (Proj09_6) A.17.1 Continuïtat de la seguretat de la informació (Proj09_3)	
Dominis de la ISO		A.4 Context de l'organització A.5 Lideratge A.9 Avaluació de l'exercici A.10 Millora	
Amenaces a tractar		[E] Errors i fallades no intencionades [A] Atacs intencionats	
Prioritat	**Planificació**	Alta	Curt termini
Cost	**Millora**	523550€	L3 – L4
Responsable		CIO, RSI, responsable SI	

Taula 44. Projecte 9 Nous procediments de SI

En aquest projecte s'ha trobat a faltar:

- Un procediment que reguli la infraestructura que han de tenir les oficines locals, tot i que si que existeix una bona pràctica, el procediment no està descrit ni alineat amb la ISO 27001. Per tant caldrà revisar totes les infraestructures i adaptar-les al compliment de la norma.
- Cal normalitzar el procediment per tal de encriptar tots els discs de portàtils i emmagatzemar i tenir una copia d'aquestes claus d'encriptació, també cal tenir procedimentats l'ús certificats.
- Cal elaborar un pla de continuïtat de negoci.
- Cal crear els procediments de contacte amb grups especials, gestió de projecte i per l'adquisició de nou components que fins ara no estan procedimentats de forma específica a l'organització.

Personal	Nº	Fase	hores	Cost	Total
CIO	1	Assignació de projectes	4	45€	180€
DPO	1		4	45€	180€
RSI	1		4	45€	180€
Resp. SI	1		4	45€	180€
Tècnic	1	Desenvolupament del procediment d'infraestructures	20	30€	600€
CIO	1	Revisió i aprovació del procediment	2	45€	90€
RSI	1		2	45€	90€
Resp. SI	1		2	45€	90€
Tècnic	1		2	30€	60€
Tècnic	4	Revisió de les instal·lacions	160	30€	19200€
Resp. SI	1	Desenvolupament de nous procediments	20	45€	900€
Tècnic	3		20	30€	1800€
Implementació d'adaptacions i millores (proveïdor)					500000€
				Total	**523550€**

Taula 45. Resum d'hores destinades al Proj09

ROI - ↓ Baix

Al igual que els projectes de formació, la realització d'aquests nous procediments son necessari pel compliment de la ISO 27001 tot i que no comporten una repercussió econòmica directa.

Projecte 10. Gestió d'actius

Nom	**ID**	Gestió d'actius		Proj10
Objectiu		Tot i que existeix un procediment, cal refer tot el procediment per tal d'adaptar-lo a la ISO 27001. Com pot ser l'eliminació, l'esborrat i la reutilització dels actius, la utilització de suports extraïbles		
Controls de la ISO		A.8 Gestió d'actius		
Amenaces a tractar		[E] Errors i fallades no intencionades		
Prioritat	**Planificació**	Alta	Curt termini	
Cost	**Millora**	37010€		L4
Responsable		Responsable SI		

Taula 46. Projecte 10 Gestió d'actius

Personal	Nº	Fase	hores	Cost	Total
CIO	1	Creació grup de treball i definició del projecte	4	45€	180€
Resp. SI	1		4	45€	180€
Resp. SI	1	Identificació i classificació d'actius	10	45€	450€
Tècnic	4		20	30€	2400€
Tècnic	4	Inventariat i etiquetatge	135	30€	16200€
Tècnic	4	Revisió i eliminació i esborrat de suports emmagatzemats	100	30€	12000€
				Material	5600€
				Total	**37010€**

Taula 47. Resum d'hores destinades al Proj10

ROI - ↔ Mig

Com els procediments anteriors, pel compliment de la ISO 27001 la realització d'aquest projecte es necessari i ajuda a minimitzar riscos. No obstant degut als pocs incidents detectats durant aquests temps, degut a les bones pràctiques per part del departament de SI i als procediments existents creiem que el ROI per aquest projecte és mig.

Projecte 11. Procediments per la contractació de personal

Nom	**ID**	Procediments per la contractació de personal		Proj11
Objectiu		Millorar els procediments de contractació		
Controls de la ISO		A.7 Seguretat relativa als recursos humans		
Amenaces a tractar				
Prioritat	**Planificació**	mitja	mig termini	
Cost	**Millora**	3250€		L3 – L4
Responsable		Director de RH		

Taula 48. Projecte 11 Procediments per la contractació de personal

Tot i que existeix un procediment de contractació i si que es fa una investigació d'antecedents en el treballadors que han de tractar amb menors, cal fer extensible aquest procediment a tots els treballadors. També cal procedimentar el procés de comunicació entre SI i RH en el canvi de responsabilitats dins l'organització, que ja es tracte en el procediments de les guies d'administradors locals.

Personal	**Nº**	**Fase**	**hores**	**Cost**	**Total**
Director RH	1	Procediments per la contractació de personal	50	45€	2250€
Tècnic RH	1		50	20€	1000€
				Total	**3250€**

Taula 49. Resum d'hores destinades al Proj11

ROI - ↓ Baix

Com en els casos anteriors, el projecte és necessari pel compliment de la ISO encara que suposi un ROI baix ja que les bones pràctiques per part del departament de RH no havia suposat cap incident de seguretat, tot i que si que existia el risc.

Millores Intrínseques

Cal indicar que amb la realització d'aquest treball ja provoquen una millora en la pròpia organització, com són la anàlisis de riscos, la política de seguretat, el procés d'auditories ... amb això provoca un millora en els Controls A.5, A.6, A.16, A.18 i la Norma 4, 5, 6, 7, 8, 9, 10.

ID	Nom		Inici	Finalització
Proj01	Campanya de conscienciació sobre la seguretat en els sistemes d'informació a l'organització		2/1/2023	29/12/2023
		Creació grup de treball i definició de campanyes	2/1/2023	6/1/2023
		Desenvolupament de les campanyes	9/1/2023	27/1/2023
		Revisió de les campanyes desenvolupades	30/1/2023	30/1/2023
		Llançament de campanyes un cop al més	31/1/2023	29/12/2023
Proj02	Formacions internes d'ús de les eines informàtiques comuns a l'organització		2/1/2023	29/12/2023
		Creació grup de treball i definició de cursos	2/1/2023	6/1/2023
		Preparació dels cursos	9/1/2023	10/2/2023
		Realització de cursos dos dies per setmana durant 4 hores	13/2/2023	29/12/2023
Proj03	Formació i cursos especialitzats per Administradors de sistema		2/1/2023	29/12/2023
		Anàlisi de necessitats	2/1/2023	13/1/2023
		Realització dels cursos	16/1/2023	29/12/2023
Proj04	Implementació nou sistema antivirus de nova generació (Crowdstrike)		1/2/2023	21/3/2023
		Reunions amb proveïdor i pla de treball	1/2/2023	21/2/2023
		Implementació del nou sistema	22/2/2023	21/3/2023
Proj05	Revisió i millora del sistema de copies de seguretat		1/3/2023	7/3/2023
Proj06	Revisió i millores del control d'accessos a àrees segures		30/1/2023	10/2/2023
Proj07	Implementació d'un MDM per la telefonía mòbil		20/2/2023	31/5/2023
		Reunió amb proveïdor i definició del projecte	20/2/2023	10/3/2023
		Establiment equip tècnic	22/2/2023	22/2/2023
		Formació de l'equip tècnic	23/2/2023	5/4/2023
		Proves de funcionament	6/4/2023	3/5/2023
		Revisió del registre de terminals amb inventari de terminals distribuïts	4/5/2023	31/5/2023
		Anàlisi de les necessitats de dispositius	20/2/2023	17/3/2023
		Recepció dels nous terminals	20/3/2023	7/4/2023
		Distribució dels nous terminals	10/4/2023	5/5/2023
Proj08	Revisió i actualització dels procediments del departament de TID		9/1/2023	10/2/2023
		Assignació de projectes	9/1/2023	13/1/2023
		Revisió i actualització dels procediments	16/1/2023	3/2/2023
		Revisió i aprovació dels procediments redactats	6/2/2023	10/2/2023
Proj09	Nous procediments del departament de SI		9/1/2023	26/5/2023
		Assignació de projectes	9/1/2023	13/1/2023
		Desenvolupament del procediment d'infraestructures	16/1/2023	20/1/2023
		Revisió i aprovació del procediment	23/1/2023	27/1/2023
		Revisió de les instal·lacions	30/1/2023	24/3/2023
		Implementació d'adaptacions i millores	27/3/2023	26/5/2023
		Desenvolupament de nous procediments	16/1/2023	3/2/2023
		Revisió i aprovació dels nous procediments redactats	6/2/2023	10/2/2023
Proj10	Gestió d'actius		20/2/2023	12/5/2023
Proj11	Creació grup de treball i definició del projecte		20/2/2023	24/2/2023

Taula 50. Planificació dels projectes

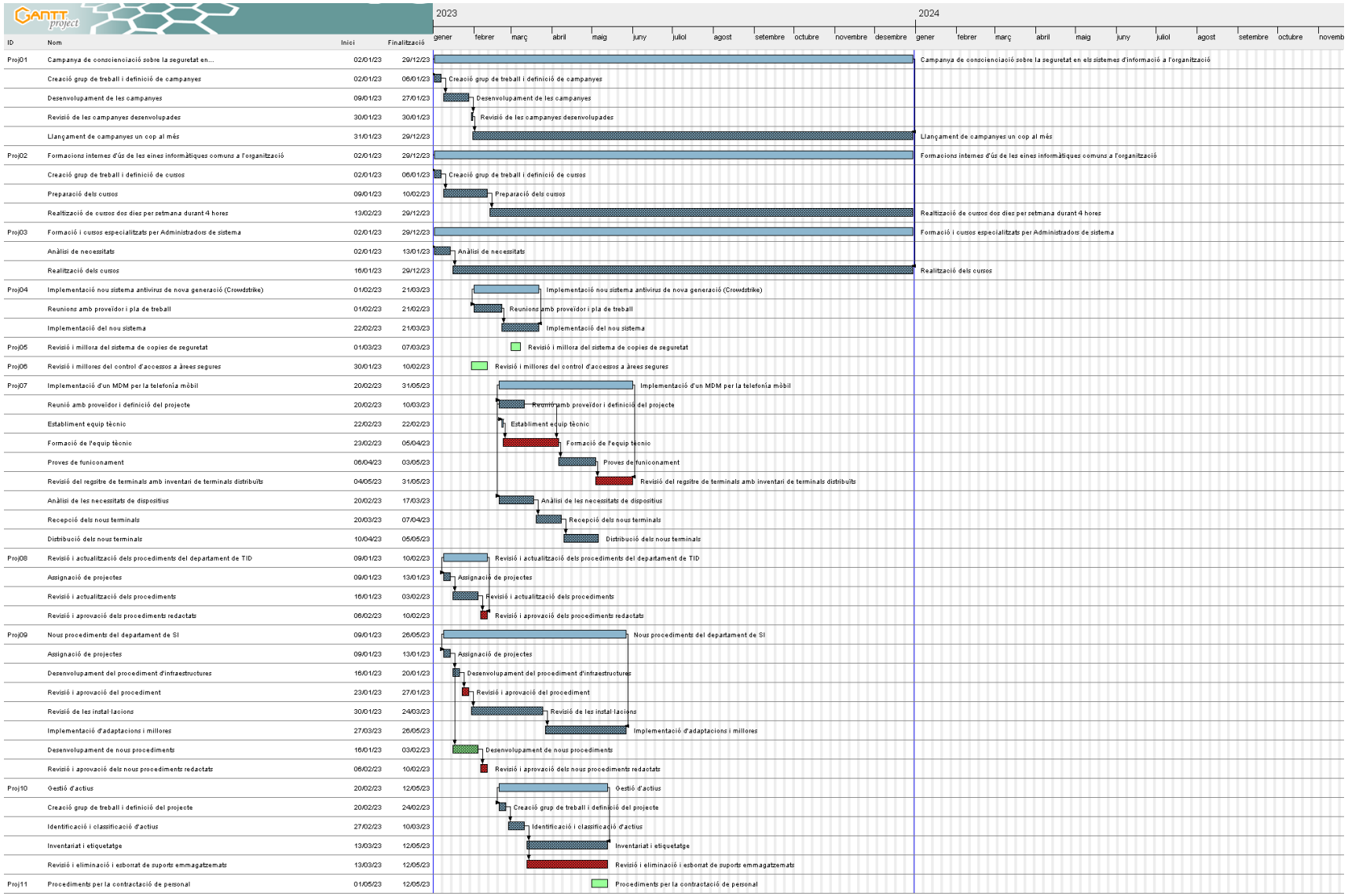

Figura 10. Diagrama de Gantt de planificació de projectes

6. Informe d'auditoria

En el procés de implementació d'un SGSI, després d'haver definit l'abast i el context on aplicar aquesta implementació, en el què hem identificat els actius i les amenaces, s'han definit els indicadors, s'ha realitzat un anàlisi del risc i definit els projectes de millora cal verificar el compliment de cadascun dels controls de la ISO 27001 i 27002 amb la finalitat de mantenir el sistema de millora continua que requereix l'SGSI, a aquesta auditoria la definim com a Auditoria de compliment i ens ha de servir per analitzar si el treball realitzat fins el moment s'ha realitzat de forma correcta.

Per tal de realitzar aquest propòsit es seguiran els procediments descrits a l'annex 2 sobre procediments d'auditoria

Com s'acaba de dir, aquesta és una auditoria de compliment interna sobre el procediment realitzat en la implementació de la norma ISO 27001, per tant, s'haurà de valorar de nou la maduresa tant de la norma com dels controls.

La realització d'aquest treball ja suposa una millora i un compliment de la Norma ISO 27001, ja que aquesta és l'objectiu de realitzar-lo, per tant no cal aprofundir molt més en aquest anàlisis que es troba mes detallat a l'annex 8, si comparem amb el nivell de maduresa inicial tenim que:

Control	Nivell de maduresa inicial	Nivell actual	Objectiu
4 L'Organització i el Context	1,75	**3,00**	**3**
5 Lideratge	2,11	**3,00**	**3**
6 Planificació	1,60	**3,00**	**3**
7 Suport	2,73	**3,73**	**4**
8 Operació	1,33	**3,17**	**3**
9 Avaluació de l'exercici	2,78	**3,61**	**4**
10 Millora	2,25	**3,50**	**4**

Taula 51. Resum valoració maduresa assolida de la norma

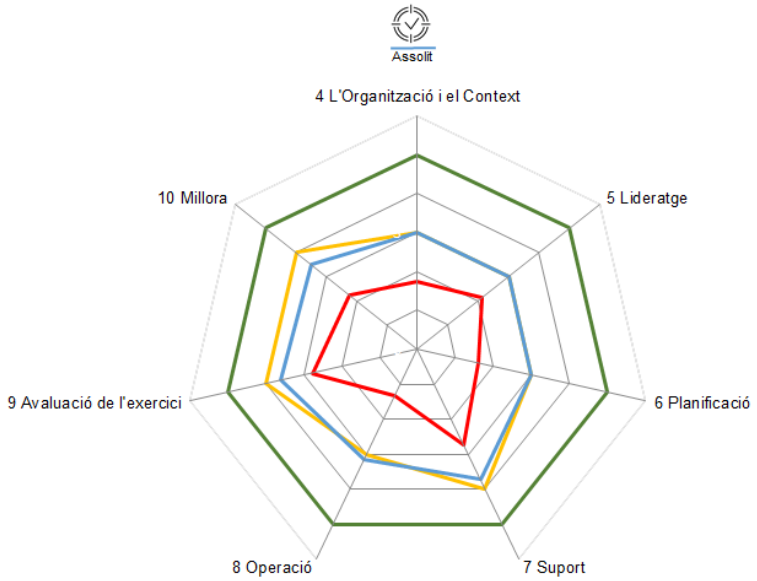

Figura 11. Nivell de maduresa de la norma assolit

Com es pot observar hi ha una millora substancial en totes les àrees.

Pel què fa als controls descrits a la ISO 27002 que trobem resumits en la taula 52 i desenvolupats a l'annex 8 també trobem una millora important, tot i no haver assolit l'objectiu en la majoria d'àrees s'ha quedat a prop.

Control	Nivell de maduresa inicial	Nivell actual	Objectiu
A.5 Polítiques de seguretat de la informació	2,00	3,50	4
A.6 Organització de la Seguretat de la informació	2,55	4,00	4
A.7 Seguretat relativa als recursos humans	2,83	3,75	3
A.8 Gestió d'actius	2,19	4,00	4
A.9 Control d'accés	2,87	3,83	4
A.10 Criptografia	2,00	3,00	3
A.11 Seguretat física i de l'entorn	2,72	3,42	4
A.12 Seguretat de les operacions	2,57	3,82	4
A.13 Seguretat de les comunicacions	3,00	3,50	4
A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació	2,78	3,67	4
A.15 Relació amb proveïdors	3,00	3,83	4
A.16 Gestió d'incidents de seguretat de la informació	2,86	3,57	4
A.17 Aspectes de seguretat de la informació per la gestió de la continuïtat del negoci	3,17	3,67	4
A.18 Compliment	2,20	3,90	4

Taula 52. Resum valoració maduresa assolida dels controls de la ISO 27002

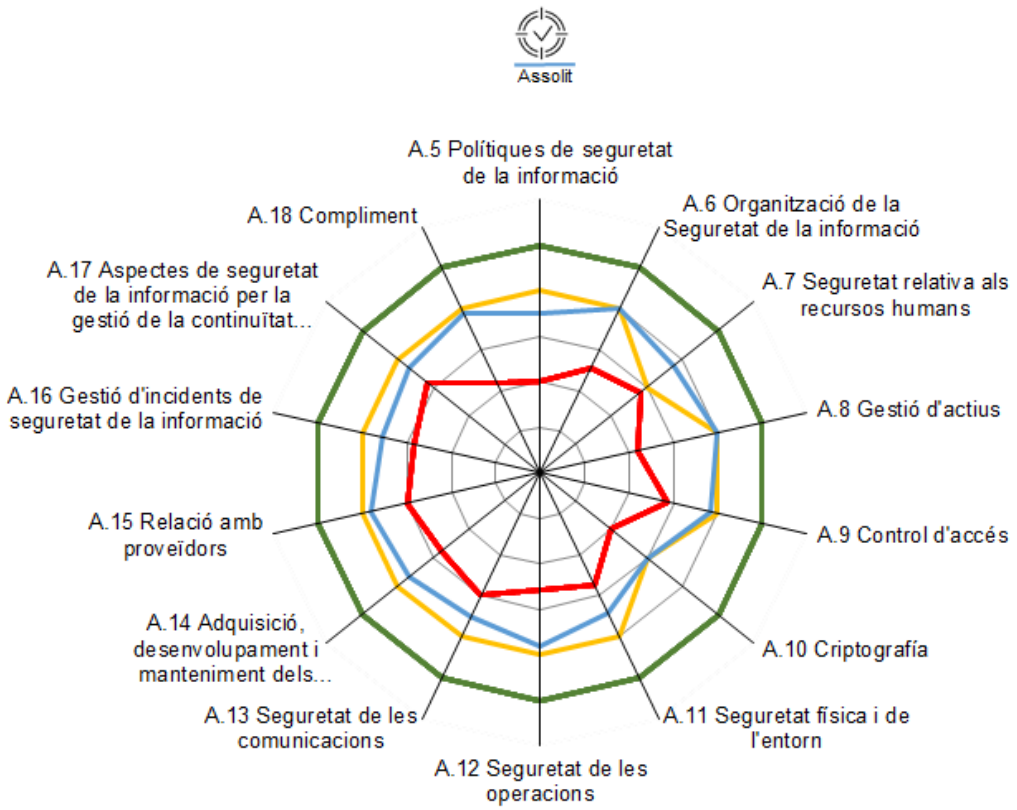

Figura 12. Nivell de maduresa dels controls assolit

Tant amb la norma com en els controls no s'ha acabat d'assolir l'objectiu fixat en un inici, no obstant la millora ha estat notable, donant compliment a totes les àrees i estar en disposició de passar una auditoria de certificació.

Pel què referència a les noves valoracions de la norma de la taula 51 cal destacar que s'han superat més del 50% dels objectius fixats en un inici, no obstant el propi procés implementat, basat en un sistema PDCA de millora continua, ens porta inexorablement a assolir aquest objectiu o inclús superar-lo en properes auditories.

Analitzant de forma global els resultats obtinguts en el nivell de maduresa dels controls, encara que tampoc s'han assolit els objectius marcats en un inici el creixement en maduresa s'ha produït de forma homogènia en totes les àrees, exceptuant l'àrea de criptografia que s'ha quedat una mica més enrere, tot i que ha assolit l'objectiu fixat juntament amb l'organització de la seguretat de la informació i la gestió d'actius, la resta d'àrees han obtingut una valoració global similar. Com en el cas de exposat en el paràgraf anterior, el propi sistema fixat en porta a assolir aquest objectiu en un curt període de temps.

D'aquest anàlisi se n'extreuen unes no conformitats, que en el cas que ens pertoca només són de caràcter menor i observacions.

Cal indicar que les no conformitats classificades com a Menor també s'haurien pogut tractar com observacions, no obstant, s'han classificat com a no conformitats pel fet que cal posar remei al punt en qüestió per poder tenir un bon compliment de la norma. Les observacions són recomanacions de millora que no

suposen un incompliment, no obstant, una reiteració continuada d'aquestes observacions i un no tractament d'aquestes podria acabar suposant una no conformitat en futures auditories.

Secció	Control	Tipus	Justificació
A.8.2.2	Etiquetatge de la informació	Observació	El projecte s'ha definit i s'ha realitzat, tot i el procés s'han detectat algunes deficiències en l'etiquetat que s'hauran de revisar de nou.
A.8.3.2	Eliminació de suports	Menor	El projecte s'ha definit i es suposa realitzat tot i que s'ha detectat dins del procediment, el temps que ha de passar per l'eliminació dels suports, també s'han detectat suports no eliminats.
A.9.1.1	Polítiques de control d' accés	Menor	Existeixen diversos procediments que recullen diferents tipus de control d'accés, és recomanable unificar en una política sobre control d'accessos que reculli tots els protocols d'accés, tot i que es poden mantenir els procediments específics destinats a conceptes concrets.
A.10.1.1	Polítiques d' ús dels controls criptogràfics	Menor	La guia de bones pràctiques recull la política d'ús de controls criptogràfics, aquest procediment s'hauria de recollir en una política específica i concreta i no com a una bona pràctica.
A.10.1.2	Gestió de Claus	Observació	S'hauria de revisar el procediment creat sobre la gestió de les claus criptogràfiques, cal entrar més al detall i definir millor el procediment.
A.11.1.3	Seguretat d' oficines, despatxos i recursos	Observació	No es recull específicament la seguretat en oficines i despatxos en els protocols
A.11.1.6	Àrees de càrrega i descàrrega	Observació	No es recull específicament la seguretat en les zones de càrrega i descàrrega
A.11.2.9	Política de lloc de treball ordenat i pantalla neta	Menor	Tot i està ben definit i recollit en tots els procediments, s'han detectat deficiències en alguns llocs de treball. Caldria un procés de revisió
A.12.1.4	Separació dels recursos de desenvolupament, prova i operació	Observació	Estan separats els entorns de prova i operació, es recullen conceptes en diferents projectes. S'hauria de crear un procediment específic per aquest control
A.14.2.8	Proves funcionals de seguretat de sistemes	Menor	S'han detectat irregularitats com són la no realització de les proves descrites en els procediments per tal d'accelerar la posada en funcionament els sistemes.
A.14.2.9	Proves d' acceptació de sistemes	Menor	S'han detectat irregularitats, petits incompliments, en aquest procediment
A.16.1.3	Notificació de punts febles de la seguretat	Observació	Tot i existir el procediment de notificació de bretxes, s'ha trobat a faltar un conscienciació entre els treballadors sobre aquest tema, també s'ha detectat poc coneixement d'aquest procediment entre els treballadors. Es recomana fer una campanya de comunicació i conscienciació enfocada a aquest punt

Taula 53. No Conformitats

Es recomana treballar en les no conformitats menors de manera immediata i seguir treballant en la línia que s'ha traçat seguint el pla de millora continuada, que permetrà aconseguir el nivell de maduresa objectiu en tots els controls de la ISO 27002 en futures auditories.

7. Conclusions

Amb la realització d'aquest treball es pretenia avançar en la millora de l'organització i dotar de un nivell de seguretat suficient a la informació de l'organització. Dona confiança i un bon servei a administracions i usuaris a sigut la prioritat d'aquesta organització. Tot i que des de la direcció i el departament de SI s'ha treballat sempre en aquest sentit, la seguretat sempre ha estat un tema que ha preocupat, ja que en el Tercer Sector es sol treballar amb informació sensible i cal preservar-la.

Cal destacar el fet que l'Organització és una ONG, amb la qual cosa els recursos dels que es disposa son limitats, i les necessitats i urgències dels moments compliquen les planificacions a mig-llarg termini. El nivell de funcionament és un altre dels factors que s'han de tenir en compte, ja que el funcionament organitzatiu és molt similar al de l'administració pública, amb això, vull dir que, sabent que el nivell d'implantació de sistemes com la ISO/IEC27001 o l'ENS en el cas de l'administració pública és molt baix, degut a les complicacions que implementar aquests mètodes comporta en aquest tipus d'organitzacions, fer-ho en la nostre organització és un gran salt qualitatiu.

Durant el desenvolupament del treball m'he adonat que l'organització havia dedicat ja molts esforços i inversions a la seguretat, però que s'havia fet una mica sobre la marxa i en funció de les necessitats del moment. Seguir un mètode com el que proposa la Norma ISO 27001, tot i que comporta un gran esforç ens garanteix uns resultats més acurats i evita treballs i inversions innecessàries i més adaptades a la realitat, en definitiva fa mes eficient els treballs i les actuacions a realitzar.

Crec que s'ha assolit gran part de l'objectiu inicial d'aquest treball on s'han fet tots els passos per la implementació d'un SGSI seguint la indicacions de la Norma ISO 27001, dic gran part i no tots els objectius, perquè ens havíem marcat un objectius de maduresa per els controls una mica ambiciosos, i no hem aconseguit arribar a aquests objectius, tot i que ens hi hem quedat molt a prop. La falta d'experiència i un temps limitat no m'ha permès aprofundir tant com m'hauria agradat en punts com la infraestructura de comunicacions. Caldrà seguir treballant, fer un seguiment i referenciar-nos en el pla de millora continua.

Amb un inici de TFM una mica accidentat, per motius personals vaig veure'm obligat a posposar l'inici del treball unes setmanes, vaig haver de planificar de nou els temps i les fases del treball, reduint i solapant els temps de les fases en qüestió, fins arribar a posar-me el dia amb l'última fase.

La implementació d'uns SGSI basat en la ISO 27001 no és un treball fàcil, l'experiència i un bon assessorament és clau, en molts moments et trobes en situacions que la falta d'experiència et fa prendre decisions o establir criteris erronis, i també, et condueix a un ritma de treball lent i ple de dubtes. Trobar-te amb incongruències amb algun dels criteris o valoracions establerts en un inici és un exemple del que ha succeït en alguna ocasió, modificar aquesta valoració inicial per poder donar congruència i sentit al desenvolupament del treball i traslladar el que es volia transmetre realment ha sigut la decisió presa.

8. Glossari

ENS Esquema Nacional de Seguretat

ONG Organització No Governamental

ISO International Organitzation for Standaritzation

IEC Comissió Electrònica internacional

MAGERIT Metodologia d'Anàlisis i Gestió de Riscos dels Sistemes de Informació

PDCA Cicle de Deming; Plan-Do-Check-Act

PDS Pla Director de Seguretat

SGSI Sistema de Gestió de la Seguretat de la Informació

Confidencialitat Només les persones autoritzades tenen accés a la informació sensible o privada.

Integritat La informació i els mètodes de processament d'aquesta informació són exactes i complets, i no s'han de modificar sense autorització.

Disponibilitat Els usuaris que hi estan autoritzats poden accedir a la informació quan ho necessitin.

9. Bibliografia

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

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

[3] **27001 Academy** - Informe: Lista de documentación obligatoria requerida por ISO/IEC 27001. Setembre de 2014. Material disponible de l'assignatura.

[4] **INCIBE** - Plan Director de Seguridad https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad 4/11/2022

[5] **MAGERIT** – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid, Octubre de 2012
Disponible al portal d'Administració electrònica (PAe): https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html 4/11/2022

[6] **UOC** – Apunts de l'assignatura M1.709 – Sistemes de gestió de la seguretat. Implantació d'un sistema de gestió de la seguretat de la informació (SGSI), PID_00275344

[7] **UOC** – Apunts de l'assignatura M1.810 – Auditoria Tècnica. Introducció a l'auditoria TIC i de seguretat TIC, PID_00239291

[8] **UOC** – Apunts de l'assignatura M1.810 – Auditoria Tècnica. Auditoria de certificació ISO 27001, PID_00239288

[9] **UOC** – Apunts de l'assignatura M1.709 – Sistemes de gestió de la seguretat. Desenvolupament d'alguns objectius de control de l'SGSI, PID_00275342

[10] Documentació empresarial pròpia

[11] **INCIBE** – CEO, CISO, CIO… ¿Roles en ciberseguridad? https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad 18/11/2022

[12] **UOC** – Apunts de l'assignatura M1.709 – Anàlisi de riscos, PID_00275340

10. Annex 1 Política de Seguretat

Organització			LOGO
Nom del document		**Codi de document**	
Política de Seguretat		PS-SI.ORG01	
Versió	**Data**	**Autor**	
1.0			

Revisat per:	Aprovat per:

D'acord amb el marc de seguretat de la informació establert per l'ONG, aquesta política defineix les obligacions i limitacions del personal, voluntari, col·laborador o tercer en quant a:

- Aplicació dels controls adequats per preservar la seguretat de la informació.
- Utilitzar els recursos i tecnologies de la informació i les comunicacions de manera eficaç, eficient o coherent amb els principis de l'ONG.
- Donar compliment al marc legal aplicable a l'activitat de l'ONG.
- Garantir la continuïtat del procés de negoci de l'ONG.
- Garantir el procés de millor continua i la revisió periòdica del SGSI.
- Garantir el coneixement i aplicació d'aquesta política per part del personal, voluntariat o tercers implicats en la prestació dels serveis de l'organització.

Tal i com s'indica en les guies d'implementació d'un PDS s'han de definir els rols i les responsabilitats sobre els actius de l'organització. Es pot trobar el detall d'aquests a l'annex 5 Gestió de rols i responsabilitats.

- L'alta direcció.
- **CIO** és el director de Tecnologies de la informació i Digitalització. (*Chief Information Office*).
- **CISO** és el director de seguretat de la informació (*Chief Information Security Officer*), la seva tasca és la de donar compliment a la política i estratègia de l'organització pel que fa referència a la seguretat de la informació.
- **DPO** és el delegat de protecció de Dades (*Data Proteccion Officer*).
- Responsable de l'Oficina de protecció de Dades.
- Responsable de seguretat de les tecnologies de la informació i Digitalització.
- Responsable del departament de Tecnologies de la informació i

Digitalització.

- Proveïdors de Serveis.
- Directors d'àmbit.
- Treballadors.
- Voluntaris.

L'ONG confereix diferents usos i destins a la informació que rep i processa, la reputació de l'ONG, així com l'eficàcia i l'eficiència de la tasca que realitza pot veure's afectada si la informació no és protegida sigui quina sigui la forma en que es comparteix, es guarda o es transmet. Per tant s'ha de garantir tant la **Confidencialitat**, la **Integritat** i la **Disponibilitat** d'aquesta, basant-se en la norma marcada a la ISO/IEC 27001.

Aquesta política de seguretat va adreçada i és d'obligat compliment per tot el personal, voluntaris i/o col·laboradors de la pròpia organització o tercers que treballin per o en nom de la organització.

Aquesta política afecta a totes les àrees de la institució, incloent els centres territorials, des dels que presten serveis essencials.

Aquesta política s'aplica a:

- Tots els treballadors, voluntaris i tercers implicats en la prestació dels serveis essencials.
- Tots els actius de la informació i dades en qualsevol format (oral, escrit, imprès, electrònic, òptic, electromagnètic, etc.) en qualsevol moment del seus cicle de vida (recol·lecció, manteniment, distribució, ús, emmagatzematge, arxivament i destrucció) propietats de l'ONG o de tercers que s'utilitzin per la prestació dels serveis.

Aquesta política de seguretat de la informació serà examinada en les revisions del sistema per la direcció a través del comitè de seguretat de la informació, sempre que es produeixin canvis significatius i/o com a mínim un cop l'any.

11. Annex 2 Procediment d'auditories internes

Organització			LOGO
Nom del document		**Codi de document**	
Procediment d'auditories internes		PAI-SI.ORG01	
Versió	**Data**	**Autor**	
1.0			

Revisat per:	Aprovat per:

Tot SGSI, incloent el basat en la ISO/IEC 27001 rau sobre la base de un sistema de millora continuada tipus PDCA (*cicle de Deming*), planificar (*Plan*), fer (*Do*), verificar (*Check*) i actuar (*Act*). És en aquesta tercera fase del cicle en que es troba el procés d'auditar internament l'SGSI [6] [7] [8].

L'auditoria té com a objectius:

- Obtenir evidències de com l'SGSI implantat compleix amb els requisits establerts i utilitzar aquestes evidències per seguir actuant en els sistema de millora continuada.
- Identificar, prevenir i corregir possibles vulnerabilitats i/o amenaces a la que la organització està exposada.

L'auditoria ha d'incloure l'abast i les àrees auditades, així com l'equip auditor. Les persones que realitzaran aquestes auditories han de tenir el perfil adequat per tal d'auditar els controls, per tant pot haver-hi més d'un perfil auditor segons els tipus de control, ja siguin més tècnics o més organitzatius.

Els rols en aquest procediment quedarien distribuïts així:

- **Auditor en Cap** és el rol principal i necessari, és el responsable final de l'auditoria. Ha de tenir coneixements del sistema a auditar. Aquest és designat per la direcció de l'organització. Formen part de les seves responsabilitats:
  - Establir els objectius, l'abast, els criteris i la durada de l'auditoria.
  - Designar l'equip auditor i tècnic necessari per portar-la a terme.
  - Assegurar-se que l'auditoria es realitzi correctament seguint el pla establert.
- **Auditor** ha de tenir coneixements específics de l'àmbit a auditar, també ha de tenir coneixement sobre la legislació aplicable i els reglaments vigents, i ha de tenir la capacitat per entendre les particularitats de l'organització auditada. Està sota la supervisió de l'auditor en cap.

- **Tècnics especialistes** seran els encarregats de realitzar algunes de les tasques tècniques quan els coneixements i l'habilitat de l'auditor no siguin suficients per realitzar una tasca específica. El tècnic sempre actuarà sota la supervisió d'un auditor.

Com ja s'ha comentat en el sistema de millora continuada tipus PDCA cal fer auditories de forma periòdica per tal és necessari fer una planificació d'aquestes seguint un criteri preestablert.

Per les característiques de la nostre organització creiem adient el següent programa d'auditories:

- Una revisió anual de conformitat del SGSI amb la norma ISO/IEC 27001.
- Una revisió anual del pla de continuïtat.
- Una auditoria trimestral dels controls de seguretat lògics.
- Una auditoria Anual dels controls de seguretat física.
- Una auditoria Biennal de protecció de dades de caràcter personal.

Referent a l'informe d'auditoria aquest ha d'incloure com a mínim els següents elements:

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

12. Annex 3 Gestió d'indicadors

Organització			LOGO
Nom del document		**Codi de document**	
Gestió d'indicadors		GI-SI.ORG01	
Versió	**Data**	**Autor**	
1.0			

Revisat per:	Aprovat per:

Tal i com està definit i explicat als apunts de l'assignatura Sistemes de Gestió de la seguretat [6], cal avaluar l'eficàcia del sistema de manera continuada, per fer-ho cal establir uns indicadors que ens permetin controlar el funcionament, l'eficàcia i l'eficiència que tenen, definir-ne els mecanismes i la periodicitat de la mesura. Aquests indicadors han de tenir com a mínim els següents components bàsics:

- Nom de l'indicador
- Descripció de l'indicador
- Control o controls de seguretat a qui dona cobertura
- Formula de mesurament
- Unitats de Mesura
- Freqüència de mesura
- Valor objectiu que és desitjable
- Valor de Tall, és el valor límit a partir del qual salta l'alarma
- Responsable de la mesura

Nom de l'indicador	Polítiques de Seguretat de la informació
Descripció	Mesura l'existència i/o revisió de les polítiques i guies de seguretat de la informació
Controls de Seguretat	A.5.1.1. Polítiques per a la seguretat de la informació A.5.1.2. Revisió de les polítiques per a la seguretat de la informació A.6.2.1. Política de dispositius mòbils A.6.2.2. Teletreball A.8.2.1. Classificació de la informació A.9.1.1. Polítiques de control d'accés A.10.1.1. Polítiques d'ús dels controls criptogràfics A.11.2.8. Equip d'usuari desatès A.11.2.9. Política de lloc de treball ordenat i pantalla neta A.12.1.1. Documentació de procediments operacionals A.12.3.1. Copies de Seguretat de la informació A.12.6.2. Restriccions en la instal·lació del programari A.13.2.1. Polítiques i procediments d'intercanvi d'informació A.13.2.2. Acords d'intercanvi d'informació A.13.2.4. Acords de confidencialitat o no revelació A.14.2.1. Polítiques de Desenvolupament segur

		A.15.1.1. Política de seguretat de la informació en les relacions amb els proveïdors A.16.1.1. Responsabilitats i procediments A.16.1.2. Notificació dels esdeveniments de seguretat de la informació	
Formula de mesurament		Quantitat de polítiques revisades respecte del total en l'últim any	
Unitat de mesurament		(Núm. De polítiques revisades / Núm. de polítiques totals)*100	
Freqüència de mesurament		Anual	
Objectiu	Tall	100%	<85%
Identificador		Ind01	
Responsable		Comitè de Seguretat de la informació	

Taula 54. Ind01 – Polítiques de Seguretat de la informació

Nom de l'indicador		Rols i Responsabilitats	
Descripció		Mesura les incidències o no conformitats en la gestió dels rols i les responsabilitats.	
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.6.2.2. Teletreball A.10.1.2. Gestió de Claus A.11.1.1. Perímetre de seguretat física A.16.1.1. Responsabilitats i procediments	
Formula de mesurament		Quantitat d'incidències reportades els últims tres mesos	
Unitat de mesurament		Recompte d'incidències reportades trimestralment	
Freqüència de mesurament		Trimestral	
Objectiu	Tall	0	<5
Identificador		Ind02	
Responsable		Comitè de Seguretat de la informació	

Taula 55. Ind02 – Rols i Responsabilitats

Nom de l'indicador		Gestió de Projectes	
Descripció		Mesura el compliment de la seguretat en la gestió de projectes	
Control de Seguretat		A.6.1.5 Seguretat de la informació en la gestió de projectes	
Formula de mesurament		Quantitat d'incidències reportades els últims tres mesos	
Unitat de mesurament		Recompte d'incidències reportades trimestralment	
Freqüència de mesurament		Trimestral	
Objectiu	Tall	0	<5
Identificador		Ind03	
Responsable		Director d'àmbit del projecte	

Taula 56. Ind03 – Gestió de Projectes

Nom de l'indicador		Procediments de Recursos Humans	
Descripció		Mesura els procediments relacionats amb el Recursos Humans	
Controls de Seguretat		A.7.1.1. Investigació d'antecedents A.7.1.2. Termes i condicions de l'ocupació A.7.2.1. Responsable de gestió A.7.2.3. Procés disciplinari A.7.3.1. Responsabilitat davant la finalització o canvi	
Formula de mesurament		Quantitat de incidències reportades en un més.	

Unitat de mesurament		Recompte d'incidències reportades mensualment	
Freqüència de mesurament		Mensual	
Objectiu	Tall	0	<5
Identificador		Ind04	
Responsable		Direcció de Recursos Humans	

Taula 57. Ind04 – Procediments de Recursos Humans

Nom de l'indicador		Formació i conscienciació	
Descripció		Mesura les campanyes de formació, conscienciació en matèria de seguretat de la informació	
Control de Seguretat		A.7.2.2. Conscienciació, educació i capacitació en seguretat de la informació	
Formula de mesurament		Quantitat de cursos i campanyes que s'han fet anualment	
Unitat de mesurament		Número de cursos i campanyes que s'han fet en un any	
Freqüència de mesurament		Anualment	
Objectiu	Tall	12	<9
Identificador		Ind05	
Responsable		Direccions d'àmbit i comitè de seguretat	

Taula 58. Ind05 – Formació i conscienciació

Nom de l'indicador		Inventari d'actius	
Descripció		Mesura que tots els actius estiguin inventariats i tinguin un responsable	
Controls de Seguretat		A.8.1.1. Inventari d'actius A.8.1.2. Propietat dels actius	
Formula de mesurament		Actius detectats no inventariats correctament sobre el total d'actius.	
Unitat de mesurament		(Núm. Equips no inventariats / Núm. Equips totals)*100	
Freqüència de mesurament		Mensual	
Objectiu	Tall	0%	>5%
Identificador		Ind06	
Responsable		Responsable de Seguretat	

Taula 59. Ind06 – Inventari d'actius

Nom de l'indicador		Control i gestió d'actius	
Descripció		Mesura el compliment de les normes d'ús	
Controls de Seguretat		A.8.1.3. Ús acceptable dels actius A.8.1.4. Devolució dels 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	
Formula de mesurament		Quantitat de incidències reportades en un més	
Unitat de mesurament		Recompte d'incidències reportades mensualment	
Freqüència de mesurament		Mensual	
Objectiu	Tall	0	<5
Identificador		Ind07	
Responsable		Responsable de Seguretat	

Taula 60. Ind07 – Control i gestió d'actius

Nom de l'indicador		Classificació de la informació	
Descripció		Mesura el compliment de les polítiques sobre classificació de la informació sobre etiquetatge i manipulació.	
Controls de Seguretat		A.8.2.2. Etiquetatge de la informació A.8.2.3. Manipulat de la informació	
Formula de mesurament		Quantitat d'incidències reportades els últims tres mesos	
Unitat de mesurament		Recompte d'incidències reportades trimestralment	
Freqüència de mesurament		Trimestral	
Objectiu	Tall	0	<5
Identificador		Ind08	
Responsable		Responsable de Seguretat	

Taula 61. Ind08 – Classificació de la informació

Nom de l'indicador		Accés a xarxes, serveis de xarxa a sistemes i aplicacions	
Descripció		Mesura les no conformitats en quant a l'accés a xarxes com a diferents sistemes i aplicacions	
Controls de Seguretat		A.9.1.2. Accés a les xarxes i als serveis de xarxa A.9.4.1. Restricció de l'accés a la informació A.9.4.5. Control d'accés al codi font dels programes A.13.1.1. Controls de xarxa A.13.1.2. Seguretat dels serveis de xarxa A.13.1.3. Segregació en xarxes A.14.2.5. Principis d' enginyeria de sistemes segurs	
Formula de mesurament		Quantitat d'accessos denegats o il·legítims sobre el total d'accessos concedits	
Unitat de mesurament		(Núm. no accessos / Núm. accessos totals)*100	
Freqüència de mesurament		Mensual	
Objectiu	Tall	0%	>10%
Identificador		Ind09	
Responsable		Responsable de Seguretat	

Taula 62. Ind09 – Accés a xarxes, serveis de xarxa a sistemes i aplicacions

Nom de l'indicador		Gestió segura d'usuaris	
Descripció		Controla que la gestió dels usuaris i privilegis sigui la correcte en cada moment	
Controls de Seguretat		A.9.2.1. Registre i baixa d'usuari A.9.2.2. Provisió d'accés d'usuari A.9.2.3. Gestió de privilegis d'accés A.9.2.6. Retirada o reassignació dels drets d'accés A.9.4.2. Procediments segurs d'inici de sessió A.9.4.4. Ús d'utilitats amb privilegis del sistema	
Formula de mesurament		Quantitat de modificacions fetes incloent altes i baixes respecte el total de altes, baixes i modificacions contractuals i voluntariat totals al llarg de un més.	
Unitat de mesurament		(Núm. de modificacions / Núm. Total)*100	
Freqüència de mesurament		Mensual	
Objectiu	Tall	100%	<85%
Identificador		Ind10	
Responsable		Direcció de Recursos Humans i Responsable de Sistemes d'informació.	

Taula 63. Ind10 – Gestió segura d'usuaris

Nom de l'indicador		Gestió de claus d'usuari segures	
Descripció		Mesura els incidents relacionats amb els accessos d'usuari, caducitats i usos.	
Controls de Seguretat		A.9.2.4. Gestió de la informació secreta d'autenticació dels usuaris A.9.2.5. Revisió dels drets d'accés d'usuari A.9.3.1. Ús de la informació secreta d'autenticació A.9.4.3. Sistemes de gestió de contrasenyes	
Formula de mesurament		Quantitat de incidents detectats en un més.	
Unitat de mesurament		Núm. de incidències detectades mensualment	
Freqüència de mesurament		Mensual	
Objectiu	Tall	0	<5
Identificador		Ind11	
Responsable		Responsable de Seguretat	

Taula 64. Ind11 – Gestió de claus d'usuari segures

Nom de l'indicador		Seguretat en les instal·lacions	
Descripció		Mesura els incidents de seguretat a les instal·lacions en un període de tres mesos	
Controls de Seguretat		A.11.1.1. Perímetre de seguretat física A.11.1.2. Controls físics d'entrada A.11.1.3. Seguretat d'oficines, despatxos i recursos A.11.1.4. Protecció contra les amenaces externes i ambientals A.11.1.5. El treball en àrees segures A.11.1.6. Àrees de càrrega i descàrrega	
Formula de mesurament		Quantitat de incidents reportats en tres mesos.	
Unitat de mesurament		Núm. de incidències detectades trimestralment	
Freqüència de mesurament		Trimestral	
Objectiu	Tall	0	<3
Identificador		Ind12	
Responsable		Direcció de Serveis Generals	

Taula 65. Ind12 – Seguretat en les instal·lacions

Nom de l'indicador		Seguretat física en els equips	
Descripció		Mesura els incidents relacionat amb la seguretat física dels equips en un període de tres mesos	
Controls de Seguretat		A.11.2.1. Emplaçament i protecció d'equips A.11.2.2. Instal·lacions de subministraments A.11.2.3. Seguretat del cablejat A.11.2.6. Seguretat dels equips fora de les instal·lacions	
Formula de mesurament		Quantitat de incidents reportats en tres mesos.	
Unitat de mesurament		Núm. de incidències detectades trimestralment	
Freqüència de mesurament		Trimestral	
Objectiu	Tall	0	<5
Identificador		Ind13	
Responsable		Responsable de Seguretat	

Taula 66. Ind13 – Seguretat física en els equips

Nom de l'indicador	Manteniment dels equips
Descripció	Mesura el nivell de manteniment dels equips
Controls de Seguretat	A.11.2.4. Manteniment dels equips

	A.11.2.7. Reutilització o eliminació segura d'equips		
Formula de mesurament	Equips que no han tingut contacte amb el sistema respecte els equips totals en els últims 6 mesos.		
Unitat de mesurament	(Equips no contactats / Equips Totals)*100		
Freqüència de mesurament	Semestral		
Objectiu	Tall	0%	>10%
Identificador	Ind14		
Responsable	Responsable de Sistemes d'informació		

Taula 67. Ind14 – Manteniment dels equips

Nom de l'indicador	Gestió de procediments operacionals		
Descripció	Mesura el nivell de revisió dels procediments operacionals relacionats amb els sistemes de la informació		
Controls de Seguretat	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 A.14.2.5. Principis d' enginyeria de sistemes segurs		
Formula de mesurament	Quantitat de procediments revisats respecte del total en l'últim any		
Unitat de mesurament	(Núm. De polítiques revisades / Núm. de polítiques totals)*100		
Freqüència de mesurament	Anual		
Objectiu	Tall	100%	<85%
Identificador	Ind15		
Responsable	Comitè de Seguretat		

Taula 68. Ind15 – Gestió de procediments operacionals

Nom de l'indicador	Desenvolupament i programari segur		
Descripció	Mesura les incidències relacionades amb el desenvolupament i instal·lació de programari		
Control(s) de Seguretat	A.12.1.4. Separació dels recursos de desenvolupament, prova i operació A.12.5.1. Instal·lació del programari en explotació A.14.2.4. Restriccions als canvis en els paquets de programari A.14.2.5. Principis d' enginyeria de sistemes segurs A.14.2.6. Entorn de desenvolupament segur A.14.2.7. Externalització del desenvolupament de programari		
Formula de mesurament	Quantitat de incidents reportats en sis mesos.		
Unitat de mesurament	Núm. de incidències detectades semestralment		
Freqüència de mesurament	Semestral		
Objectiu	Tall	0	<5
Identificador	Ind16		
Responsable	Responsable de Seguretat		

Taula 69. Ind16 – Desenvolupament i programari segur

Nom de l'indicador	Atacs i Vulnerabilitats
Descripció	Mesura la quantitat de incidents (codi maliciós, vulnerabilitats, incidents de correu, ...) tractats de seguretat detectats respecte al total d incidents detectats al llarg d'un més
Control(s) de Seguretat	A.12.2.1. Controls contra el codi maliciós A.12.6.1. Gestió de les vulnerabilitats tècniques A.13.2.3. Missatgeria electrònica A.14.1.2. Assegurar els serveis d' aplicacions en xarxes públiques

	A.14.1.3. Protecció de les transaccions de serveis d' aplicacions		
Formula de mesurament	Quantitat de incidents tractats en un més respecte al total de incidents detectats en un més		
Unitat de mesurament	(Núm. De incidents tractats / Núm. de incidents totals)*100		
Freqüència de mesurament	Mensual		
Objectiu	Tall	100%	90%
Identificador	Ind17		
Responsable	Responsable de Seguretat		

Taula 70. Ind17 – Atacs i Vulnerabilitats

Nom de l'indicador	Processos de registres i auditories		
Descripció	Mesura l'existència del compliment de les normes relacionades amb els registres i les auditories		
Control(s) de Seguretat	A.12.4.1. Registres d' esdeveniments 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 A.12.7.1. Controls d' auditoria de sistemes d' informació A.17.1.3. Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació A.18.2.1. Revisió independent de la seguretat de la informació A.18.2.3. Comprovació del compliment tècnic		
Formula de mesurament	Existeixen les normes o estàndards?		
Unitat de mesurament	Si=1 – NO=0		
Freqüència de mesurament	Anual		
Objectiu	Tall	1	0
Identificador	Ind18		
Responsable	Responsable de Seguretat		

Taula 71. Ind18 – Processos de registres i auditories

Nom de l'indicador	Requisits i processos de millora		
Descripció	Mesura l'existència dels anàlisis dels requisits i els processos de millora en els processos dels sistemes de informació		
Control(s) de Seguretat	A.14.1.1. Anàlisi de requisits i especificacions de seguretat de la informació A.16.1.3. Notificació de punts febles de la seguretat A.16.1.4. Avaluació i decisió sobre els esdeveniments de seguretat d' 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		
Formula de mesurament	Existeixen els requisits i processos?		
Unitat de mesurament	Si=1 – NO=0		
Freqüència de mesurament	Anual		
Objectiu	Tall	1	0
Identificador	Ind19		
Responsable	Responsable de Seguretat		

Taula 72. Ind19 – Requisits i processos de millora

Nom de l'indicador	Entorn de prova
Descripció	Mesura el compliment de l'estàndard relacionat amb l'entorn de proves

Control(s) 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	
Formula de mesurament		Es compleix amb l'estàndard?	
Unitat de mesurament		Si=1 – NO=0	
Freqüència de mesurament		Anual	
Objectiu	Tall	1	0
Identificador		Ind20	
Responsable		Responsable de Seguretat	

Taula 73. Ind20 – Entorn de prova

Nom de l'indicador		Relació amb proveïdors	
Descripció		Mesura el compliment de la política de seguretat en les relacions amb els proveïdors	
Control(s) 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 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	
Formula de mesurament		Es compleix la política?	
Unitat de mesurament		Si=1 – NO=0	
Freqüència de mesurament		Anual	
Objectiu	Tall	1	0
Identificador		Ind21	
Responsable		CIO	

Taula 74. Ind21 – Relació amb proveïdors

Nom de l'indicador		Pla de continuïtat de Negoci	
Descripció		Mesura el grau de compliment del pla de continuïtat de negoci	
Control(s) de Seguretat		A.17.1.1. Planificació de la continuïtat de la seguretat de la informació A.17.1.2. Implementar la continuïtat de la seguretat de la informació A.17.2.1. Disponibilitat dels recursos de tractament de la informació	
Formula de mesurament		Quantitat de mesures implantades respecte a les mesures planificades	
Unitat de mesurament		(Núm. Mesures implantades / Núm. Mesures planificades)*100	
Freqüència de mesurament		Anual	
Objectiu	Tall	100%	<85%
Identificador		Ind22	
Responsable		Comitè de Seguretat	

Taula 75. Ind22 – Pla de continuïtat de Negoci

Nom de l'indicador	Anàlisi de Compliment
Descripció	Mesura el grau de compliment legal, contractual i de les polítiques i normes de seguretat
Control(s) 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 l' organització A.18.1.4. Protecció i privacitat de la informació de caràcter personal A.18.1.5. Regulació dels controls criptogràfics A.18.2.2. Compliment de les polítiques i normes de seguretat

Formula de mesurament		Es compleix?	
Unitat de mesurament		Si=1 – NO=0	
Freqüència de mesurament		Anual	
Objectiu	Tall	1	0
Identificador		Ind23	
Responsable		Comitè de Seguretat	

Taula 76. Ind23 – Anàlisi de Compliment

13. Annex 4 Procediment de revisió per direcció

Organització			LOGO
Nom del document		**Codi de document**	
Procediment de revisió per direcció		PRD-SI.ORG01	
Versió	**Data**	**Autor**	
1.0			

Revisat per:	Aprovat per:

Tal i com indica la norma ISO/IEC 27001 [1] en el seu punt 9.3, l'alta direcció ha de revisar el sistema de gestió de la seguretat de la informació en intervals planificats, per assegurar la seva conveniència, adequació i eficàcia continua.

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

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

L'informe resultant de la revisió ha d'incloure les decisions relacionades amb les oportunitats de millora i qualsevol necessitat de canvi en l'SGSI.

S'ha de conservar informació documentada com a evidència de les revisions fetes per part de la direcció.

Aquestes revisions s'han de realitzar de forma periòdica i en cap cas poden superar l'any entre revisions. En el cas de que es produeixi un canvi substancial en alguns dels requeriments que afecten l'SGSI caldrà una nova revisió.

Els participants en les revisions poden ser variables en funció de les parts interessades en cada moment, no obstant sempre ha d'estar format per:

- Direcció.
- CIO.
- CISO.

Altres participants a criteri de la direcció poden ser:

- Responsable de la oficina de protecció de dades.
- Responsable de Seguretat de sistemes de la informació.
- Responsables de Sistemes i Tecnologies de la informació.
- Altres responsables i directors de departament.

14. Annex 5 Gestió de rols i responsabilitats

Organització			LOGO
Nom del document		**Codi de document**	
Gestió de rols i responsabilitats		GRR-SI.ORG01	
Versió	**Data**	**Autor**	
1.0			

Revisat per:	Aprovat per:

Existeixen diferents rols i responsabilitats de la informació en la implementació d'un SGSI per tal de desenvolupar les polítiques, procediments, regles i controls necessaris.

En aquest sentit també existeix el comitè de seguretat de la informació (CSI), format per alguns dels rols que s'aniran descrivint al llarg d'aquest annex [9][10][11].

El comitè de seguretat està format per:

CIO és el director de Tecnologies de la informació i Digitalització. (*Chief Information Office*). La seves funcions principal són:

- Procurar que les estratègies de l'organització estiguin alineades amb la tecnologia de la informació per assolir els objectius planificats.
- Millorar els processos de les tecnologies de la informació.
- Promoure i coordinar entre les àrees de negoci l'anàlisi de riscos dels processos més crítics i la informació més sensible, i proposar accions per a millorar i mitigar el risc, d'acord amb el llindar acceptable que ha definit el comitè de direcció. Elevar el mapa de riscos i el pla de seguretat de la informació al comitè de seguretat de la informació (CSI).
- Coordinar el comitè de seguretat.

CISO és el director de seguretat de la informació (*Chief Information Security Officer*), la seva tasca és la de donar compliment a la política i estratègia de l'organització pel que fa referència a la seguretat de la informació.

- Elaborar, promoure i mantenir una política de seguretat de la informació i proposar anualment objectius en matèria de seguretat de la informació.
- Vetllar pel compliment legal i coordinar les actuacions necessàries amb les unitats responsables.
- Desenvolupar i mantenir el document d'Organització de la seguretat de la informació en col·laboració amb l'àrea d'organització o recursos humans, en el qual es recull qui assumeix cadascuna de les

responsabilitats en seguretat i també una descripció detallada de funcions i dependències.

- Vetllar pel compliment legal i coordinar les actuacions necessàries amb les unitats responsables.
- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.
- Controlar la gestió de riscos de nous projectes i vetllar pel desenvolupament segur d'aplicacions.

Responsable de l'Oficina de protecció de Dades és el responsable d'assessorar, supervisar, monitoritzar el compliment de la normativa vigent en quant a protecció de dades

RSI Responsable de seguretat dels sistemes de la informació i Digitalització.

- Implantar les directrius del comitè de seguretat de la informació de la companyia.
- Desenvolupar, amb el suport de les unitats corresponents, el marc normatiu de seguretat i controlar-ne el compliment.
- Actuar com a punt focal en matèria de seguretat de la informació dins de la companyia, cosa que inclou la coordinació amb altres unitats i funcions (seguretat física, prevenció, emergències, relacions amb la premsa, etc.), a fi de gestionar la seguretat de la informació de manera global.
- Revisar periòdicament l'estat de la seguretat en qüestions organitzatives, tècniques o metodològiques. Aquesta revisió ha de permetre proposar o actualitzar el pla de seguretat de la informació i incorporar-hi totes les accions preventives, correctives i de millora que s'han anat detectant. Una vegada el CSI ha aprovat aquest pla i el pressupost, l'RSI ha de gestionar el pressupost assignat i la contractació de recursos quan sigui necessari.
- Definir l'arquitectura de seguretat dels sistemes d'informació, monitorar la seguretat en l'àmbit tecnològic (gestió de traces, vulnerabilitats, canvis, etc.), fer el seguiment de les incidències de seguretat i escalar-les al CSI si correspon.
- Elaborar i mantenir un pla de conscienciació i formació en seguretat de la informació del personal, en col·laboració amb la unitat responsable de formació de la companyia.
- Fer el seguiment de les incidències de seguretat, revisar-les i escalar-les al CSI si correspon.
- Coordinar la implantació d'eines i controls de seguretat de la informació i definir el quadre de comandament de la seguretat. L'RSI ha d'analitzar i mantenir actualitzat aquest quadre de comandament i presentar-lo al CSI amb la periodicitat que s'estableixi.

Tot i que pot esta format puntualment per altres rols a demanda del comitè, aquests rols són els següents:

DPO és el delegat de protecció de Dades (*Data Proteccion Officer*) en el nostre cas és un proveïdor de serveis que assessora al Responsable de la oficina de protecció de dades en quant a la protecció de dades.

Responsable del departament de Tecnologies de la informació i Digitalització és els responsable tècnic del departament de Tecnologies de la informació en tots els àmbits que no estan relacionats amb la seguretat

Directors d'àmbit són els màxims responsables en cadascun dels àmbit de l'organització i els responsables de que els treballadors, voluntaris i proveïdors de serveis propis estiguin informats, formats i complexin amb les directrius en quan a la seguretat dels sistemes de la informació

Proveïdors de Serveis tenen la obligació de complir amb les directrius de l'organització en quant a la seguretat dels sistemes de informació durant tot els períodes i processos del servei. També tenen la obligació d'informar sobre possibles incidents de seguretat o vulnerabilitats detectades.

Treballadors tenen la obligació de conèixer la política de seguretat de la informació així com totes les altres polítiques i normes en qüestió de seguretat. També tenen la obligació d'informar sobre possibles incidents de seguretat o vulnerabilitats detectades.

Voluntaris Tenen les mateixes responsabilitats que els treballadors en quan a la seguretat dels sistemes de la informació

En quan a les responsabilitats d'aquest comitè són:

- Establir les polítiques de seguretat corporativa que hauran de ser aprovades per la direcció.
- Coordinar totes les funcions de seguretat de l'organització.
- Vetllar pel compliment de la normativa legal i sectorial d'aplicació vigent.
- Vetllar per què les activitats de seguretat estiguin alineades amb els objectius de l'organització.
- Coordinar els plans de continuïtat de negoci.
- Coordinar i aprovar les propostes de projectes en els diferents àmbits de la seguretat, essent l'encarregat de gestionar un control, supervisar el progrés dels projectes i les seves possibles derivacions.
- Rebre les inquietuds de la direcció en qüestió de seguretat i transmetre-la als responsables pertinents, i transmetre les possibles respostes i solucions d'aquests i comunicar-les a la direcció.
- Recopilar informes regulars de l'estat de la seguretat dels diferents responsables de seguretat dels departaments.

- Coordinar i donar resposta a les consultes dels diferents responsables de seguretat departamentals i/o la direcció.
- Definir l'assignació de rols i responsabilitats i els criteris per garantir una bona praxis en la segregació de funcions.
- Informar regularment a la direcció.
- Promoure la millora continua del SGSI.
- Elaborar l'estratègia de l'organització en les qüestions de la seguretat de la informació.
- Coordinar els esforços en matèria de seguretat de la informació per assegurar que estan alineats amb l'estratègia decidida i evitar esforços duplicats.
- Elaborar i revisar regularment la política de seguretat de la informació per tal de que sigui aprovada per la direcció.
- Aprovar la normativa de seguretat de la informació.
- Elaborar i aprovar els requisits de formació i qualificació dels administradors, operadors i usuaris des del punt de vista de la seguretat de la informació.
- Monitoritzar els principals riscos residuals que s'assumeixen per part de l'organització i recomanar-ne possibles actuacions.
- Monitoritzar el desenvolupament dels processos de gestió de incidents de seguretat i recomanar-ne possibles actuacions.
- Promoure la realització d'auditories periòdiques que permetin verificar el compliment del SGSI.
- Aprovar plans de millora de la seguretat que es puguin portar a terme des de diferents àmbits..
- Prioritzar les actuacions en seguretat quan els recursos siguin limitats
- Vetllar per que en tots els projecte TIC es tingui present la seguretat de la informació en tot el seu cicle de vida
- Resoldre els conflictes de responsabilitat entre diferents responsables i/o àrees de l'organització, o elevar-los a la direcció en el cas que sigui necessari.

El comitè tindrà reunions ordinàries de forma trimestral i com a mínim se n'hauran de fer tres a l'any. No obstant, el mateix comitè podrà decidir la convocatòria de reunions tants cops com sigui necessari per tal de complir amb els seus propòsits.

S'ha d'aixecar acte dels temes tractats a les reunions del comitè per tal de deixar documentat per futures consultes i revisions.

15. Annex 6 Metodologia d'anàlisi de riscos

Organització			LOGO
Nom del document		**Codi de document**	
Metodologia d'anàlisi de riscos		MAR-SI.ORG01	
Versió	**Data**	**Autor**	
1.0			

Revisat per:	Aprovat per:

Les pautes d'implementació d'un anàlisi segons trobem a [6] han de ser:

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

En el nostre cas utilitzarem la metodologia Magerit [5][12]. Que diu que l'anàlisi de riscos es una aproximació metòdica per determinar els risc seguint una sèrie de passes pautades:

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

No obstant a aquests passos tindríem una fase prèvia que seria la de recol·lecció de dades i processos de informació i dimensionament i establiment de paràmetres.

Fase 0 Presa de dades i establiment de paràmetres

Aquesta fase prèvia, de fet, és la més important de tota la metodologia, ja que és en la que es defineix l'abast, en funció d'aquest abast el procés serà més o menys costos, i quan més abast més gran serà el nombre de riscos.

Un altre factor a tenir en compte, és que s'han d'analitzar els processos que realitza l'organització, ja que els riscos que puguin aparèixer poden interferir en aquests processos.

En aquesta fase prèvia també s'han d'establir els paràmetres que s'utilitzaran durant tot el procés de l'anàlisi de riscos. Aquests paràmetres són:

- Valor dels actius.
- Vulnerabilitat.
- Impacte.
- Efectivitat del control de seguretat.

Fase 1 Valoració d'actius

Aquesta fase és en la que s'identifiquen aquells actius que són importants per l'organització, tenint en compte que en els sistemes de informació hi ha dues coses essencials, la informació i els serveis que s'ofereixen.
Segons la metodologia escollida, Magerit, classificarien els actius així:

- Dades (D).
- Claus Criptogràfiques (KY).
- Serveis (S).
- Aplicacions informàtiques (SW).
- Equips informàtics (HW).
- Suports de informació (MED).
- Equipament auxiliar (AUX).
- Xarxes de comunicació (COM).
- Instal·lacions (L).
- Persones (P).

La dependència entre actius és un fet a destacar, la informació i els serveis prestats són els actius essencials, no obstant aquests depenen d'altres més prosaics, com poden ser equips, instal·lacions, comunicacions, ... Això implica que la materialització d'una amenaça en un actiu inferior té conseqüències en un de superior. L' esquema de dependència del actius vindria a ser:

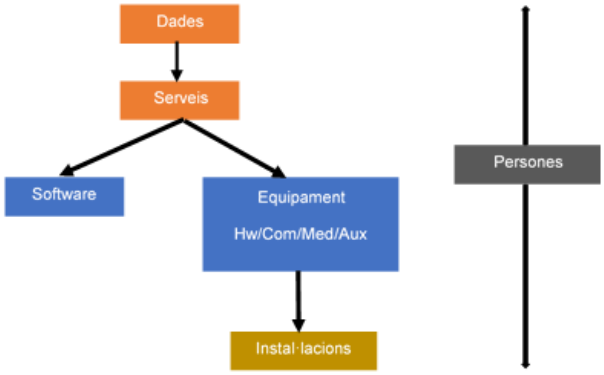

Figura 13. Dependències entre actius

Dels actius també ens interessa calibrar les diferents dimensions com són la:

- Confidencialitat (C)
- Integritat (I)
- Disponibilitat (D)
- Autenticitat (A)
- Traçabilitat (T)

Quan es fa la valoració dels actius no nomes es té el valor de compra de l'actiu, sinó que també s'ha de tenir en compte quin és el valor segons la importància que té per la tasca que realitza. Per tal de dur a terme aquesta valoració s'han d'establir diferents rangs segons el valor que tenen, les recomanacions és que no s'utilitzin més de cinc rangs [12][5]. Seguint aquests criteris els possibles valors que tindrem seran els següents:

Valoració		Rang	Valor
Molt Alt	MA	Valor >200000€	300000€
Alt	A	100000€ < valor > 200000 €	150000€
Mig	M	50000€ < valor > 100000 €	75000€
Baix	B	10000€ < valor > 50000 €	30000€
Molt Baix	MB	valor < 10000 €	10000€

Taula 77. Valor dels actius

A més, per valorar les diferents dimensions escollirem una escala detallada de 10 valors, seguint la recomanació anterior de no utilitzar més de cinc rangs, adaptem la taula que trobem al llibre 3 de Magerit [5], deixant els següents valors:

Valor		
Molt Alt	MA	10 9
Alt	A	8 7
Mig	M	6 5 4
Baix	B	3 2
Molt Baix	MB	1 0

Taula 78. Valoració de les dimensions

Fase 2 Anàlisi d'amenaces, vulnerabilitats i impactes

S'han de determinar les amenaces que poden afectar a cada actiu, una amenaça és quelcom que pot succeir, i el que ens interessa és allò que pot causar-li un dany. Les amenaces es poden classificar com:

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

Un cop determinat que una amenaça pot perjudicar un actiu, s'ha de valorar la seva influència en el valor de l'actiu en dos sentits:

- Degradació – quan perjudicat resultaria el valor del actiu
- Probabilitat – quan probable o improbable és que es materialitzi l'amenaça

La degradació es sol caracteritzar amb una fracció del valor de l'actiu, per aquest motiu seguirem els criteris següents:

Degradació		
Molt Alta	MA	100%
Alta	A	75%
Mitja	M	50%
Baixa	B	20%
Molt Baixa	MB	5%

Taula 79. Valoració de la degradació

La probabilitat d'ocurrència es més complexa de determinar i expressar, nosaltres ens decantarem pel model numèric, tal i com es mostra en la taula següent:

Probabilitat				
Molt freqüent	Diària	MA	5	100
Freqüent	Mensualment	A	4	10
Normal	Anualment	M	3	1
Poc freqüent	Varis anys	B	2	0,10
Molt poc freqüent	Segles	MB	1	0,01

Taula 80. Probabilitat d'ocurrència

L'impacte és la mesura del dany sobre l'actiu derivat de la materialització d'una amenaça. Coneixent el valor dels actius en les diferents dimensions i la degradació que causen les amenaces se'n deriva l'impacte sobre el sistema.

Fase 3 Estimar l'impacte

En aquest punt hem de determinar quin serà l'impacte potencial que es tindria si es materialitzes qualsevol de les amenaces.

L'impacte no és més que el producte del valor de l'actiu per la degradació que pateix l'actiu si una amenaça es materialitza. A la següent taula podem veure els nivells d'impacte definits

Impacte (Valor x Degradació)		
Molt Alt	MA	10 9
Alt	A	8 7
Mig	M	6 5 4
Baix	B	3 2
Molt Baix	MB	1 0

Taula 81. Impacte

Fase 4 Determinació del risc

El risc és el càlcul resultant del producte de l'impacte potencial amb la probabilitat de que una amenaça es materialitzi.

La taula següent mostra els valors de que es tindran en compte per determinar el risc real i el risc acceptable.

Taula de Risc							
Impacte	MA	10	10	20	30	40	50
		9	9	18	27	36	45
	A	8	8	16	24	32	40
		7	7	14	21	28	35
	M	6	6	12	18	24	30
		5	5	10	15	20	25
		4	4	8	12	16	20
	B	3	3	6	9	12	15
		2	2	4	6	8	10
	MB	1	1	2	3	4	5
		0	0	0	0	0	0
			1	2	3	4	5
			MB	B	M	A	MA
			Probabilitat				

Taula 82. Risc

En funció de la valoració que surti s'haurà de valorar quin tractament s'ha de fer d'aquest risc, així que si la valoració es igual o menor a 15 l'organització assumirà el risc i si és més gran en funció de l'amenaça i l'actiu aquest es podrà mitigar o reduir, eliminar o derivar cap a un tercer.

En aquest punt definim cal que definim els termes següents:

Risc real: És el risc al que esta exposat tenint en compte totes les mesures de seguretat existents en el moment.

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

Nivell de risc acceptable: És el nivell a partir del qual l'organització està disposada acceptar el risc i no portar a terme cap acció correctiva o mitigadora.

16. Annex 7 Declaració d'aplicabilitat

Organització			LOGO
Nom del document		**Codi de document**	
Declaració d'aplicabilitat		DA-SI.ORG01	
Versió	**Data**	**Autor**	
1.0			

Revisat per:	Aprovat per:

A la normativa ISO/IEC 27001 ve definit que les organitzacions han de determinar quins són els controls necessaris dins de l'abast del SGSI i fer-ne una declaració d'aplicabilitat que contingui, els controls necessaris, la justificació de la inclusió o no i si els controls estan implementats o no [1].

Secció	Control	Justificació	Aplicabilitat	Estat Actual	Nivell de compliment	Observacions
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 a la seguretat de la informació	Existeixen una sèrie de normatives com poden ser: La normativa de protecció de dades, ús dels equips, ús del correu electrònic, guies de protecció de dades, guies d'orientació sobre l'ús de missatgeria com per exemple whatsapp. Procediment de l'exercici del dret.	Aplica	incomplert	2	No existeix una política de seguretat definida, però si una series de normatives, guies i polítiques, però estan incompletes
A.5.1.2	Revisió de les polítiques per a la seguretat de la informació		Aplica	incomplet	2	
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.	Estan definits rols i les responsabilitats però no dins d'un pla global.	Aplica	cal revisar i actualitzar	3	Cal revisar, actualitzar i desenvolupar aquells procediments conforme la ISO 27001 que guarden relació amb l'Organització interna de l'organització sobre rols, responsabilitats, segregació de tasques, ... No estan inclosos dins d'una política de seguretat.
A. 6.1.2	Segregació de tasques.	En la gestió dels rols i responsabilitats també existeix un protocol de segregació de tasques	Aplica	cal revisar i actualitzar	3	
A. 6.1.3	Contacte amb les autoritats.	Existeix un procediment de notificació de	Aplica	cal revisar i actualitzar	3	

		bretxes de seguretat				
A. 6.1.4	Contacte amb grups d' interès especial.	No existeix un procediment específic per aquest tipus de contacte amb grups especials	Aplica	Pendent	2	
A.6.1.5	Seguretat de la informació en la gestió de projectes.	No existeix un procediment específic per la seguretat en la gestió de projectes	Aplica	Pendent	2	
A.6.2	Els dispositius mòbils i el teletreball.					
A.6.2.1	Política de dispositius mòbils.	No hi ha una guia específica sobre mòbils, però si sobre missatgeria.	Aplica	Pendent	2	Cal desenvolupar el procediment conforme la ISO 27001
A.6.2.2	Teletreball.	Existeix una guia sobre Teletreball	Aplica	cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment que reculli tot l'abast en compliment de la ISO 27001
A.7	Seguretat relativa als recursos humans					
A.7.1	Abans de l' ocupació.					
A.7.1.1	Investigació d' antecedents.	Es fa aquesta investigació a les persones que treballen amb menors. La resta no es fa.	Aplica	Implementat, cal revisar i actualitzar	2	Cal revisar i actualitzar el procediment que reculli tot l'abast en compliment de la ISO 27001
A.7.1.2	Termes i condicions de l' ocupació.	Es tenen polítiques internes i acords de confidencialitat i normatives de protecció de dades	Aplica	Implementat, cal revisar i actualitzar	3	
A.7.2	Durant l' ocupació.					
A.7.2.1	Responsabilitats de gestió.	Es tenen polítiques internes i acords de confidencialitat i normatives de protecció de dades	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment que recull tot l'abast en compliment de la ISO 27001, especialment els deures i responsabilitat dels llocs de treball en quant a la seguretat de la informació. També un procediment que controli i reculli les accions formatives realitzades
A.7.2.2	Conscienciació, educació i capacitació en seguretat de la informació.	Es realitzen accions formatives i guies pel personal, tot i que s'han detectat moltes deficiències	Aplica	Implementat, cal revisar i actualitzar	3	
A.7.2.3	Procés disciplinari.	Estan incloses en les polítiques internes de l'organització	Aplica	Implementat, cal revisar i actualitzar	3	
A.7.3	Finalització de l' ocupació o canvi de lloc de treball.					
A.7.3.1	Responsabilitat davant la finalització o canvi.	Estan inclosos en els acords de confidencialitat	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment que reculli tot l'abast en compliment de la ISO 27001
A.8	Gestió d'actius					
A.8.1	Responsabilitat sobre els actius.					
A.8.1.1	Inventari d' actius.	L'inventari existent només està referit als equips informàtics,	Aplica	Pendent	2	Cal un inventari amb tots els elements en el que es detalli tota la informació, valor,

		ordinadors i servidors, però no la resta d'actius.				propietari i responsable
A.8.1.2	Propietat dels actius.	Existeix una assignació en els actius inventariats, però amb bastantes deficiències	Aplica	Pendent	2	
A.8.1.3	Ús acceptable dels actius.	Existeix una normativa sobre l'ús dels equips	Aplica	Incomplert	3	Cal desenvolupar el procediment conforme la ISO 27001. No estan inclosos dins d'una política de seguretat.
A.8.1.4	Devolució d' actius.	Està inclosa en la normativa d'ús dels actius, però amb deficiències	Aplica	Implementat, cal revisar i actualitzar	2	Cal revisar i actualitzar el procediment que reculli tot l'abast en compliment de la ISO 27001
A.8.2	Classificació de la informació.					
A.8.2.1	Classificació de la informació.	La informació que afecte a dades personals es troba recollida en un registre d'activitats del tractament, però no existeix cap altre tipus de classificació	Aplica	Pendent	1	Cal un procediment que reculli tot l'abast en compliment de la ISO 27001 (identificació de la documentació, legalitat aplicable respecte la mateixa)
A.8.2.2	Etiquetatge de la informació.	Els suports de dades s'etiqueten per la conservació i custodia, però cal un procediment	Aplica	Implementat, cal revisar i actualitzar	2	Cal una revisió del procediment per adequar-lo a la ISO 27001. El procediment ha de recollir amb detall les mesures aplicades i el mecanismes per l'etiquetat que s'aplicaran a tots els actius
A.8.2.3	Manipulat de la informació.	Existeix un procediment d'alta i baixa d'usuaris a les aplicacions, però cal ampliar i millorar	Aplica	Implementat, cal revisar i actualitzar	2	El procediment és antic i cal una revisió i una actualització i adaptació a la ISO 27001
A.8.3	Manipulació dels suports.					
A.8.3.1	Gestió de suports extraïbles.	Existeix una guia de recomanacions i bones pràctiques on es recull el xifrat de dades i emmagatzemament de suports extraïbles, però existeixen deficiències.	Aplica	Implementat, cal revisar i actualitzar	2	El procediments són antics i cal una revisió i una actualització i adaptació a la ISO 27001
A.8.3.2	Eliminació de suports.	Existeix un procediment establert per la destrucció d'equips informàtics i esborrat i destrucció de suports de dades. En el cas de mitjans no electrònics es fa ús de destructores. Tot i que s'ha	Aplica	Implementat, cal revisar i actualitzar	3	

		detectat alguna deficiència				
A.8.3.3	Suports físics en trànsit.	Els suports de copies de seguretat són enviats fora a un proveïdor extern	Aplica	Implementat, cal revisar i actualitzar	3	
A.9	Control d'accés					
A.9.1	Requisits de negoci per al control d' accés.					
A.9.1.1	Polítiques de control d' accés	Es disposa d'un procediment de gestió d'altes d'usuari, els permisos són assignats en correspondència a les funcions a realitzar	Aplica	Implementat, cal revisar i actualitzar	3	Cal desenvolupar el procediment atenent les exigències de la ISO 27001 que reculli els requisits necessaris per accedir als diferents recursos de xarxa, aplicacions i plataformes, fitxers i registres de configuració prèvia identificació i autenticació
A.9.1.2	Accés a les xarxes i als serveis de xarxa.		Aplica	Implementat, cal revisar i actualitzar	3	
A.9.2	Gestió d' accés d' usuari.					
A.9.2.1	Registre i baixa d' usuari	Els usuaris queden identificats en polítiques a través de directori actiu, polítiques a través de les plataformes d'aplicacions i de correu O365. No obstant hi ha deficiències en la comunicació de les baixes d'usuaris	Aplica	Implementat, cal revisar i actualitzar	2	El procediment és antic i cal una revisió i una actualització i adaptació a la ISO 27001, cal posar èmfasi en recollir el procediment de comunicació entre departaments
A.9.2.2	Provisió d' accés d' usuari.	Es defineix una política de mínim privilegi, que permet que els usuaris tinguin accés als recursos pel desenvolupament de les seves activitats, també es disposa del procediment d'alta d'usuari	Aplica	Implementat, cal revisar i actualitzar	3	Cal desenvolupar el procediment conforme la ISO 27001 i en reculli tot l'abast identificant els responsables per assignar i revocar drets d'accés
A.9.2.3	Gestió de privilegis d' accés.		Aplica	Implementat, cal revisar i actualitzar	3	
A.9.2.4	Gestió de la informació secreta d' autenticació dels usuaris.	S'estableixen restriccions per l'ús de les claus de seguretat i directives de contrasenyes en el directori actiu, aplicacions i correu. No es permet l'ús compartit de claus d'accés.	Aplica	Implementat, cal revisar i actualitzar	3	Cal un procediment que reculli tot l'abast en compliment de la ISO 27001. Cal disposar d'un llistat de sistemes que recullin l'autenticació i el mecanisme corresponent.
A.9.2.5	Revisió dels drets d' accés d' usuari.	S'estableixen caducitats en les claus d'accés, però	Aplica	Implementat, cal revisar i actualitzar	3	Cal desenvolupar el procediment conforme la ISO 27001 i en

A.9.2.6	Retirada o reassignació dels drets d' accés.	existeix una deficiència de comunicació de baixes d'usuari també es detecta falta de comunicació en la revisió i retirada de drets d'accés	Aplica	Implementat, cal revisar i actualitzar	2	reculli tot l'abast identificant els responsables per assignar i revocar drets d'accés
A.9.3	Responsabilitat de l' usuari.					
A.9.3.1	Ús de la informació secreta d' autenticació.	S'estableixen restriccions per l'ús de les claus de seguretat i directives de contrasenyes en el directori actiu, aplicacions i correu. No es permet l'ús compartit de claus d'accés.	Aplica	Implementat, cal revisar i actualitzar	3	Cal un procediment que reculli tot l'abast en compliment de la ISO 27001. Cal disposar d'un llistat de sistemes que recullin l'autenticació i el mecanisme corresponent.
A.9.4	Control d' accés a sistemes i aplicacions.					
A.9.4.1	Restricció de l'accés a la informació.	Els permisos són assignats en correspondència a les funcions a realitzar	Aplica	Implementat, cal revisar i actualitzar	3	El procediment és antic i cal una revisió i una actualització i adaptació a la ISO 27001.
A.9.4.2	Procediments segurs d' inici de sessió.	S'estableixen restriccions per l'ús de les claus de seguretat i directives de contrasenyes en el directori actiu, aplicacions i correu. No es permet l'ús compartit de claus d'accés, també s'incorporen pantalles informatives on s'accepten les condicions de privacitat	Aplica	Implementat, cal revisar i actualitzar	3	El procediment és antic i cal una revisió i una actualització i adaptació a la ISO 27001.
A.9.4.3	Sistemes de gestió de contrasenyes.	S'estableixen restriccions per l'ús de les claus de seguretat i directives de contrasenyes en el directori actiu, aplicacions i correu	Aplica	Implementat, cal revisar i actualitzar	3	Cal un procediment que reculli tot l'abast en compliment de la ISO 27001. Cal disposar d'un llistat de sistemes que recullin l'autenticació i el mecanisme corresponent.
A.9.4.4	Ús d' utilitats amb privilegis del sistema.	Els permisos són assignats en correspondència a les funcions a realitzar	Aplica	Implementat, cal revisar i actualitzar	3	El procediment és antic i cal una revisió i una actualització i adaptació a la ISO 27001.
A.9.4.5	Control d' accés al codi font dels programes.	Els desenvolupaments es realitzen sobre una plataforma de desenvolupament aplicant metodologies conegudes. Tot i que s'han detectat aplicacions en centres territorials i locals fora d'aquest control	Aplica	Implementat, cal revisar i actualitzar	2	El procediment és antic i cal una revisió i una actualització i adaptació a la ISO 27001.

A.10	Criptografia					
A.10.1	Controls criptogràfics.					
A.10.1.1	Polítiques d' ús dels controls criptogràfics.	Xarxes i clients VPN per les connexions remotes. Plataformes web amb xifrat de les comunicacions. Existeix una normativa de recomanacions i bones pràctiques que recull l'enviament de documents xifrats o protegits amb claus d'accés a través de correu electrònic. Les copies de seguretat també estan xifrades	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment conforme la ISO 27001
A.10.1.2	Gestió de Claus	No existeix cap procediment al respecte	Aplica	Pendent	1	Cal incloure aquesta gestió en la política d'ús dels controls criptogràfics
A.11	Seguretat física i de l'entorn					
A.11.1	Àrees segures.					
A.11.1.1	Perímetre de seguretat física.	Existeixen varis CPDs amb control d'accés, també arxius amb informació confidencial amb control d'accés, tancats i amb climatització pròpia es disposa de càmeres de seguretat en els centres amb gravació d'imatge	Aplica	Implementat, cal revisar i actualitzar	3	S'ha d'establir un procediment que sigui d'aplicació per tots els centres que requereixen de CPD, en compliment de la ISO 27001 on s'especifiqui la necessitat de tenir àrees separades, un registre d'accés i tots els dispositius dels que es disposa. Cal un anàlisi del risc. També es requereix d'un procediment que reculli la disposició dels cartells informatius, col·locació d'extintors i ús de material inflamable, càmeres de seguretat, ...
A.11.1.2	Controls físics d' entrada.		Aplica	Implementat, cal revisar i actualitzar	3	
A.11.1.3	Seguretat d' oficines, despatxos i recursos.		Aplica	Implementat, cal revisar i actualitzar	3	
A.11.1.4	Protecció contra les amenaces externes i ambientals.		Aplica	Implementat	3	
A.11.1.5	El treball en àrees segures.		Aplica	Implementat, cal revisar i actualitzar	3	
A.11.1.6	Àrees de càrrega i descàrrega.	Es disposa de càmeres de seguretat en els centres amb gravació d'imatge	Aplica	Implementat	3	
A.11.2	Seguretat dels equips.					
A.11.2.1	Emplaçament i protecció d' equips.	Els CPDs estan ubicats en locals independents amb accés controlat en la seu central i territorial, però no sempre succeeix en els centre locals.	Aplica	Pendent	2	Cal un procediment que reculli tot l'abast en compliment de la ISO 27001 i que reculli els element adequats i la potència necessària en cada cas i que reculli el mecanisme de control que serà

A.11.2.2	Instal·lacions de subministrament.	Els CPD's disposen de SAI i climatització redundada, les oficines locals disposen de SAI per l'armari rack però no tots els centres disposen de SAI per la resta d'equips.	Aplica	Implementat	3	utilitzat per recollir i identificar les persones que accedeixen al CPD.
A.11.2.3	Seguretat del cablejat.	Els CPDs estan ubicats en locals independents amb accés controlat en la seu central i territorial, però no sempre succeeix en els centre locals.	Aplica	Pendent	2	
A.11.2.4	Manteniment dels equips.	Es preparen els equips amb una maqueta aprovada pel departament de Sistemes, aplicant les mesures de seguretat pertinent. Es disposen de servidors d'actualitzacions per minimitzar riscos. Però es detecten deficiències.	Aplica	Pendent	2	Es requereix un procediment conforme les exigències de la ISO 27001 i que indiqui quan han de ser d'aplicació les actualitzacions de seguretat i la obligació dels responsables de mantenir-se informats dels defectes i bretxes de seguretat publicades.
A.11.2.5	Retirada de materials de l' empresa.	Existeix un inventari d'equips i una política de renovació i retirada dels equips. Però existeixen algunes deficiències	No aplica	No aplica	3	Degut a l'ús massiu de portàtils i dispositius de telefonía mòbil no existeix una normativa específica, si que existeix un guia d'ús de dispositius. La seguretat dels equips ve implementada com els dispositius dins les instal·lacions.
A.11.2.6	Seguretat dels equips fora de les instal·lacions.	Existeix l'inventari i l'assignació de l'actiu, però no es fa un seguiment dels equips	No Aplica	Implementat, cal revisar i actualitzar	2	
A.11.2.7	Reutilització o eliminació segura d' equips.	Existeix un procediment establert per la destrucció d'equips informàtics i esborrat i destrucció de suports de dades	Aplica	Implementat, cal revisar i actualitzar	3	Es requereix d'una revisió del procediment per adequar-lo a les exigències de la ISO 27001, en quines circumstàncies es realitza l'esborrat i qui l'ha de realitzar
A.11.2.8	Equip d' usuari desatès.	Existeix una política per inactivitat a través de polítiques de domini.	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar el procediment que reculli els mecanismes utilitzats, temps d'inactivitat, necessitat de desbloqueig amb clau ...
A.11.2.9	Política de lloc de treball ordenat i pantalla neta.	El personal coneix la política de lloc de treball net. Però existeixen moltes deficiències i no es fa un seguiment correcte	Aplica	Implementat, cal revisar i actualitzar	2	Cal revisar el procediment que reculli la política de lloc de treball net i el seu compliment en tots els llocs de treball
A.12	Seguretat de les operacions					
A.12.1	Procediments i responsabilitats operacionals.					

A.12.1.1	Documentació de procediments operacionals.	S'han establert diferents procediments de seguretat com poden ser el pla de manteniment, pla de proves, pla de seguiment i control de millores, seguiment d'incidents, gestió de crisis, llistats de procediments per serveis, alta i baixa d'usuaris, procediments de copies de seguretat, guia d'administradors territorials de si i procediment de gestió d'incidències	Aplica	Implementat, cal revisar i actualitzar	3	Existeixen varis procediments, però cal revisar-los i actualitzar-los i adequar-los al compliment de la ISO 27001. També caldria realitzar els procediments que calgui i que en aquest moment no estiguin procedimentals
A.12.1.2	Gestió de canvis.	Es preparen els equips amb una maqueta aprovada pel departament de Sistemes, aplicant les mesures de seguretat pertinent per disminuir el risc; tot i que existeixen deficiències en alguns centres.	Aplica	Implementat, cal revisar i actualitzar	2	Cal revisar i actualitzar el procediment conforme les exigències de la ISO 27001. Generar unes maquetes generals per tots els equips amb un perfil de seguretat definit. Incloent telèfons mòbils
A.12.1.3	Gestió de capacitats.	La direcció i l'àrea de sistemes decideixen les necessitats dels nous components en funció dels volums de tractament i la qualitat dels serveis. Hi ha un pla de contingències que inclou un pla de proves, seguiment i millores. S'han incorporat mesures per evitar atacs de denegació de servei.	Aplica	Pendent	2	Cal procedimental conforme la ISO 27001 com cal recollir i identificar les necessitats dels mitjans (mitjans addicionals o capacitats dels mitjans existents, de manera que aquests satisfacin els requisits establerts), recollir la càrrega que pot suportar el sistema tenint en compte el dimensionat i la gestió de les capacitat on es detallin les mesures preventives i reactives davant atacs de denegació de servei.
A.12.1.4	Separació dels recursos de desenvolupament, prova i operació.	Existeixen procediments on es recullen les etapes d'implementació i posada en producció dels softwares desenvolupats per l'organització, les proves es realitzen en entorns aïllats i segurs	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar els procediments existents i verificar que s'ajusten als requeriments de la ISO 27001 on es detallin els plans de prova a realitzar abans que les aplicacions passin a producció. Els desenvolupaments de software han de ser objecte d'aprovació i han de seguir una metodologia definida i aprovada. El procediment ha de recollir revisions i proves prèvies realitzades.

A.12.2	Protecció contra el programari maliciós (malware).					
A.12.2.1	Controls contra el codi maliciós.	El departament de sistemes i els responsables de seguretat instal·len i gestionen els antivirus als equips i servidors i verifiquen l'actualització periòdica. S'han detectat deficiències en alguns territoris	Aplica	Implementat, cal revisar i actualitzar	2	Cal revisar i actualitzar el procediment conforme les exigències de la ISO 27001, el procediment ha de recollir les particularitats dels equips per la seva aplicació i monitorització. Cal revisar i actualitzar l'eina corporativa d'implementació de programa antivirus, anti-espia i malware
A.12.3	Còpies de seguretat.					
A.12.3.1	Còpies de seguretat de la informació.	Es realitzen copies de seguretat encriptades seguint el procediment de copies de seguretat. Es realitzen copies de seguretat sistemàtiques en tots els CPDs. A més el CPD de la oficina central es un CPD d'alta disponibilitat Actiu-Actiu	Aplica	Implementat	3	Cal evolucionar el procediment per millorar l'eficiència i tenir uns indicadors optimitzats.
A.12.4	Registres i supervisió.					
A.12.4.1	Registres d' esdeveniments.	Està activat el control de logs tant en servidors com en aplicacions corporatives. Es realitzen anàlisis periòdics per detectar incidències de seguretat. També es disposa de sistemes de detecció d'intrusions (IDS/IPS).	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment conforme l'ISO 27001 on es reculli que s'ha de registrar totes les activitats del sistema i identificant els mecanismes per registrar les activitats
A.12.4.2	Protecció de la informació del registre.	Els registres d'activitat estan protegits i només estan accessibles pels responsables de seguretat	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment que recull el període de retenció, incloent el de les evidències després de incidents
A.12.4.3	Registres d' administració i operació.	Està activat el control de logs tant en servidors com en aplicacions corporatives. Es realitzen anàlisis periòdics per detectar incidències de seguretat. També es disposa de sistemes de detecció d'intrusions (IDS/IPS).	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment conforme l'ISO 27001 on es reculli que s'ha de registrar totes les activitats del sistema i identificant els mecanismes per registrar les activitats

A.12.4.4	Sincronització del rellotge.	Els equips i servidors estan sincronitzats a una únic servidor.	Aplica	Implementat	3	
A.12.5	Control del programari en explotació.					
A.12.5.1	Instal·lació del programari en explotació.	Existeixen procediments on es recullen les etapes d'implementació i posada en producció dels softwares desenvolupats per l'organització, les proves es realitzen en entorns aïllats i segurs	*Aplica*	*Implementat, cal revisar i actualitzar*	*3*	*Cal revisar els procediments existents i verificar que s'ajusten als requeriments de la ISO 27001 on es detallin els plans de prova a realitzar abans que les aplicacions passin a producció. Els desenvolupaments de software han de ser objecte d'aprovació i han de seguir una metodologia definida i aprovada. El procediment ha de recollir revisions i proves prèvies realitzades.*
A.12.6	Gestió de la vulnerabilitat tècnica.					
A.12.6.1	Gestió de les vulnerabilitats tècniques.	Existeixen procediments on es recullen les etapes d'implementació i posada en producció dels softwares desenvolupats per l'organització, les proves es realitzen en entorns aïllats i segurs	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar els procediments d'alta i baixa d'usuaris i l'assignació de permisos per defecte així com els procediments d'actualitzacions de sistemes operatius i aplicacions.
A.12.6.2	Restricció en la instal·lació del programari.	La instal·lació està restringida per defecte en el procediment d'alta i baixa d'usuaris.	Aplica	Implementat, cal revisar i actualitzar	2	
A.12.7	Consideracions sobre l' auditoria de sistemes d' informació.					
A.12.7.1	Controls d' auditoria de sistemes d' informació.	S'han realitzat auditories de seguretat externes per saber l'estat de seguretat del sistema i les aplicacions.	Aplica	Incomplert	2	Cal implementar un procediment acord amb la ISO 27001 per la implementació d'auditories internes de la seguretat dels sistemes de la informació
A.13	Seguretat de les comunicacions					
A.13.1	Gestió de la seguretat de les xarxes.					
A.13.1.1	Controls de xarxa.	Procediment d'alta i baixa d'usuaris a les aplicacions; Punts d'accés a internet amb internet d'alta disponibilitat, Firewall, control del tràfic e/s, identificació de ports i serveis necessaris. El nivell de maduresa del	Aplica	Implementat, cal revisar i actualitzar	3	Es requereix un procediment que reculli tot l'àmbit en compliment de la ISO 27001,ha de recollir el detall dels sistemes instal·lats, l'estructura de xarxa, els punts d'interconnexió, els segments i la seva delimitació, i ha d'estar reflectida a l'estructura de seguretat del
A.13.1.2	Seguretat dels serveis de xarxa.		Aplica	Implementat, cal revisar i actualitzar	3	

A.13.1.3	Segregació en xarxes.	CPD central és alt, però hi ha deficiències en altres CPDs territorials. Utilització de xarxes i canals VPN per les connexions exteriors. Plataformes web amb xifrat de comunicacions. Separació de les xarxes de producció i desenvolupament i la xarxa DMZ per serveis externs mitjançant dispositius de Firewall	Aplica	Implementat	4	sistema on es recollirà també la segregació de xarxes.
A.13.2	Intercanvi d' informació.					
A.13.2.1	Polítiques i procediments d' intercanvi d' informació.	Polítiques i procediments descrits en tots els punts anteriors que recullen parts dels procediments, però no existeix un específic només aquest procediment	Aplica	Pendent	2	Cal implementar un procediment específic acord amb la ISO 27001 que reculli els procediments d'intercanvi d'informació.
A.13.2.2	Acords d' intercanvi d' informació.	S'incorporen als contractes amb proveïdors l'abast dels serveis. Es tenen documentats els serveis contractats amb els nivells de disponibilitat i persones de contacte.	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment que recull les mesures que s'adopten per exercir responsabilitats i manteniment del control sobre els serveis externs contractats i característiques dels riscos associats, entre d'altres
A.13.2.3	Missatgeria electrònica.	Correu corporatiu O365 gestionat pel departament de sistemes central amb mesures anti-spam i anti-malware. Existeix una normativa d'ús del correu electrònics i procediments d'enviament de documentació adjunta.	Aplica	Implementat	4	
A.13.2.4	Acords de confidencialitat o no revelació.	Es tenen polítiques internes i acords de confidencialitat i normatives de protecció de dades	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment que reculli tot l'abast en compliment de la ISO 27001
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.	La direcció i l'àrea de sistemes decideixen les necessitats dels nous components	Aplica	Incomplert	2	Cal implementar el procediment formal per planificar l'adquisició de nous components. Aquest procediment guarda

						relació directa amb l'anàlisi del risc que marcarà les prioritats
A.14.1.2	Assegurar els serveis d' aplicacions en xarxes públiques.	Plataformes web amb xifrat de comunicacions. Separació de les xarxes de producció i desenvolupament i la xarxa DMZ per serveis externs mitjançant dispositius de Firewall	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment que recull l'arquitectura de seguretat i que reflexa tots els punts d'interconnexió entre tots els sistemes i que en garanteixi l'autenticitat
A.14.1.3	Protecció de les transaccions de serveis d' aplicacions.	Es disposa d'un repositori de certificats a Azure que permet la datació del temps	Aplica	Implementat, cal revisar i actualitzar	3	
A.14.2	Seguretat en el desenvolupament i en els processos de suport.					
A.14.2.1	Política de desenvolupament segur.	Els desenvolupaments es realitzen sobre una plataforma de desenvolupament aplicant metodologies conegudes. Si tracten dades de caràcter personal es sotmeten a avaluació de l'impacte a la privacitat. Es realitzen auditories de seguretat per conèixer les possibles vulnerabilitats i vectors d'atac per prevenir incidents de seguretat. Tot i que s'han detectat aplicacions en centres territorials i locals fora d'aquest control	Aplica	Implementat, cal revisar i actualitzar	2	El procediment és antic i cal una revisió i una actualització i adaptació a la ISO 27001.
A.14.2.2	Procediment de control de canvis en sistemes.	Es preparen els equips amb una maqueta aprovada pel departament de Sistemes, aplicant les mesures de seguretat pertinent per disminuir el risc; Es disposen de servidors d'actualitzacions per minimitzar riscos tot i que existeixen deficiències en alguns centres.	Aplica	Implementat, cal revisar i actualitzar	2	Cal revisar i actualitzar el procediment conforme les exigències de la ISO 27001. Generar unes maquetes generals per tots els equips amb un perfil de seguretat definit. Incloent telèfons mòbils
A.14.2.3	Revisió tècnica de les aplicacions després d' efectuar canvis en el sistema operatiu.		Aplica	Implementat, cal revisar i actualitzar	2	

A.14.2.4	Restriccions als canvis en els paquets de programari.	s defineix una política de mínim privilegi, que permet que els usuaris tinguin accés als recursos pel desenvolupament de les seves activitats, però no realitzar canvis en el programari	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar els procediments d'alta i baixa d'usuaris i l'assignació de permisos per defecte així com els procediments d'actualitzacions de sistemes operatius i aplicacions.
A.14.2.5	Principis d' enginyeria de sistemes segurs.	Es realitzen actualitzacions de seguretat i control de ports i serveis.	Aplica	Implementat, cal revisar i actualitzar	3	El procediment és antic i cal una revisió i una actualització i adaptació a la ISO 27001.
A.14.2.6	Entorn de desenvolupament segur.	Descrit en el punt 14.2.1	Aplica	Implementat, cal revisar i actualitzar	3	
A.14.2.7	Externalització del desenvolupament de programari.	El desenvolupament de programari propi és intern i està subjecte al descrit en punts anteriors, Si es subcontracte haurà de seguir els procediments establerts per l'organització	No Aplica	Implementat, cal revisar i actualitzar	3	
A.14.2.8	Proves funcionals de seguretat de sistemes.	Es té un procediment on es recullen les etapes d'implementació i la posada en producció del softwares desenvolupats, i les proves es realitzen en entorns aïllats i segures	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar els procediments existents i verificar que s'ajusten a la ISO 27001. S'han de detallar els plans de prova a realitzar abans que les apps passin a producció. Els desenvolupaments de software han de ser objecte d'aprovació i han de seguir una metodologia definida i aprovada. El procediment ha de recollir revisions i proves prèvies realitzades.
A.14.2.9	Proves d' acceptació de sistemes.		Aplica	Implementat, cal revisar i actualitzar	3	
A.14.3	Dades de prova.					
A.14.3.1	Protecció de les dades de prova.	Queden protegides per la plataforma de desenvolupament.	Aplica	Implementat, cal revisar i actualitzar	3	Es recull en el procediment anterior
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'incorpora en els contractes amb els proveïdors l'abast dels serveis i es disposa d'un document amb els serveis contractats amb els nivells de disponibilitat i les persones de contacte.	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment que recull les mesures que s'adopten per exercir responsabilitats i manteniment del control sobre els serveis externs contractats i característiques dels riscos associats, entre d'altres
A.15.1.2	Requisits de seguretat en contractes amb tercers.		Aplica	Implementat, cal revisar i actualitzar	3	
A.15.1.3	Cadena de subministrament de tecnologia de la informació i de les comunicacions.		Aplica	Implementat, cal revisar i actualitzar	3	

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.	El departament de sistemes és l'encarregat de vetllar pel correcte funcionament diari dels serveis i establir els mecanismes de control	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment conforme a les exigències de la ISO 27001 amb el protocol d'actuació en cas d'incompliment o degradació de la qualitat dels serveis contractats i que guarda relació directa amb la gestió d'incidents
A.15.2.2	Gestió de canvis en la provisió del servei del proveïdor.		Aplica	Implementat, cal revisar i actualitzar	3	
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.	Existeix un procediment de notificació de bretxes i un procediment d'exercici de drets.	Aplica	Incomplert	2	Cal acabar de desenvolupar el procediment conforme la ISO 27001 sobre les responsabilitats i els procediments
A.16.1.2	Notificació dels esdeveniments de seguretat de la informació.	L'àrea de sistemes gestiona els incident de seguretat i posa en funcionament les mesures necessàries per la resolució. Es disposa d'una aplicació pel registre de les incidències i s'assignen les incidències a persones responsables per donar resposta i es manté un control i seguiment	Aplica	Implementat, cal revisar i actualitzar	3	Cal actualitzar i revisar el procediment conforme a la ISO 27001 en que es recull com fer front a un incident amb l'impacte en la seguretat del sistema, que recull l'actualització especial a realitzar en cas de que es requereixi de l'aïllament de l'equip i posterior anàlisi de la incidència per investigar les causes. També ha de recollir totes les actuacions realitzades en la gestió de les incidències conforme les exigències de la ISO 27001
A.16.1.3	Notificació de punts febles de la seguretat.		Aplica	Implementat, cal revisar i actualitzar	3	
A.16.1.4	Avaluació i decisió sobre els esdeveniments de seguretat d' informació.		Aplica	Implementat, cal revisar i actualitzar	3	
A.16.1.5	Resposta a incidents de seguretat de la informació.		Aplica	Implementat, cal revisar i actualitzar	3	
A.16.1.6	Aprenentatge dels incidents de seguretat de la informació.		Aplica	Implementat, cal revisar i actualitzar	3	
A.16.1.7	Recopilació d' evidències.		Aplica	Implementat, cal revisar i actualitzar	3	
A.17	Aspectes de seguretat de la informació per 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.	Es té definit un pla de contingència tecnològica o s'incorporen rols i responsabilitats dins del pla, seguiment i continuïtat dels serveis amb el seu corresponent pla de proves, control i seguiment. Però manca un anàlisi d'impacte	Aplica	Pendent	1	Cal la realització d'un anàlisi d'impacte i anàlisi del risc, que reculli tot el sistema d'informació (actius i serveis) conforme als requeriments de la ISO 27001 i programar les seves successives revisions i actualitzacions. Identificar les funcions i responsabilitats i que contingui el procediment del comitè de seguretat i crisi i la freqüència d'execució del pla de proves.
A.17.1.2	Implementar la continuïtat de la seguretat de la informació.		Aplica	Implementat, cal revisar i actualitzar	3	
A.17.1.3	Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.		Aplica	Implementat, cal revisar i actualitzar	3	

A.17.2	Redundàncies.					
A.17.2.1	Disponibilitat dels recursos de tractament de la informació.	Es disposa d'un CPD en modalitat Actiu-Actiu en alta disponibilitat. Es garanteix la disponibilitat de persones que realitzaran les tasques essencials en cas de falta del personal habitual. Generalment es disposa de mitjans alternatius per la substitució d'equips en cas de fallada. Totes les comunicacions estan redundades	Aplica	Implementat	4	
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.	Existeixen procediments de de seguretat però no es té una política de seguretat detallada i aprovada per l'organització	Aplica	Pendent	1	Cal crear una política de Seguretat en línia a la ISO 27001
A.18.1.2	Drets de Propietat Intel·lectual (DPI).		Aplica	Implementat, cal revisar i actualitzar	2	Cal revisar i actualitzar la majoria de procediments existents i adequar-los a la ISO 27001 ja que són una mica antics
A.18.1.3	Protecció dels registres de l' organització.		Aplica	Implementat, cal revisar i actualitzar	2	
A.18.1.4	Protecció i privacitat de la informació de caràcter personal.	S'han identificat els tractament de dades personals al sistema i es realitzen auditories de protecció de forma periòdica.	Aplica	Implementat	4	Realitzat
A.18.1.5	Regulació dels controls criptogràfics.	Existeix el repositori de certificats, Les copies de seguretat estan xifrades, la transferència de dades a l'exterior també estan xifrades, (vpn-https).	Aplica	Implementat, cal revisar i actualitzar	3	Cal revisar i actualitzar el procediment conforme la ISO 27001
A.18.2	Revisions de la seguretat de la informació.					
A.18.2.1	Revisió independent de la seguretat de la informació.	Com ja hem anat comentat existeixen varis procediments, polítiques i normes, però existeixen deficiències en els tres punts	Aplica	Incomplet	2	Cal acabar de desenvolupar el procediment conforme la ISO 27001
A.18.2.2	Compliment de les polítiques i normes de seguretat.		Aplica	Incomplet	2	
A.18.2.3	Comprovació del compliment tècnic.		Aplica	Incomplet	2	

Taula 83. Declaració d'aplicabilitat

17. Annex 8 Anàlisi de maduresa i compliment

Secció	Requeriment	NC inicial	NC assolit	Nivell objectiu	Projecte
4	Context de l'organització	**1,75**	**3,00**	**3**	
4.1	Comprensió de la organització i el seu context	**2,00**	**3,00**		
4.1.1	Estan identificats els objectius del SGS Sistema de Gestió de la Seguretat de la Informació?	2,00	3,00		Millores intrínseques; Proj08; Proj09
4.1.2	S'han identificat les qüestions internes i externes relacionades amb la seguretat de la informació?	2,00	3,00		Millores intrínseques; Proj08; Proj09
4.1.3	S'han identificat com les parts internes i externes poden suposar amenaces o riscos per a la seguretat de la informació?	2,00	3,00		Millores intrínseques; Proj08; Proj09
4.2	Comprensió de les necessitats i expectatives de les parts interessades	**3,00**	**3,00**		
4.2.1	S'han identificat les parts interessades?	3,00	3,00		Millores intrínseques; Proj08; Proj09
4.2.2	Hi ha un llistat de requisits sobre Seguretat de la Informació de les parts interessades?	3,00	3,00		Millores intrínseques; Proj08; Proj09
4.2.3	Hi ha un llistat de requisits sobre Seguretat de la Informació referent a reglaments, requisits legals i requisits contractuals?	3,00	3,00		Millores intrínseques; Proj08; Proj09
4.3	Determinació de l'abast del SGSI	**1,00**	**3,00**		
4.3.1	S'ha determinat l'abast del SGSI i se'n conserva informació documentada?	1,00	3,00		Millores intrínseques; Proj08; Proj09
4.4	Sistema de gestió del SGSI	**1,00**	**3,00**		
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?	1,00	3,00		Millores intrínseques; Proj08; Proj09
5	Lideratge	**2,11**	**3,00**	3	
5.1	Lideratge i compromís	**2,33**	**3,00**		
5.1.1	S'han establert objectius de la Seguretat de la Informació d'acord amb els objectius del negoci?	2,00	3,00		Millores intrínseques; Proj08; Proj09
5.1.2	La direcció proveeix dels recursos materials i humans necessaris per al compliment dels objectius del SGSI?	3,00	3,00		Millores intrínseques; Proj08; Proj09
5.1.3	La direcció revisa directament l'eficàcia de l'SGSI per garantir que es compleixen els objectius de l'SGSI?	2,00	3,00		Millores intrínseques; Proj08; Proj09
5.2	Política	**1,00**	**3,00**		
5.2.1	S'ha definit una política de seguretat de la informació?	1,00	3,00		Millores intrínseques; Proj08; Proj09
5.2.2	S'ha establert un marc que permeti establir objectius?	1,00	3,00		Millores intrínseques; Proj08; Proj09
5.2.3	S'ha comunicat la política de seguretat de la informació a les parts interessades i a tota l'empresa?	1,00	3,00		Millores intrínseques; Proj08; Proj09

5.2.4	Es manté informació documentada de la política de l'SGSI i dels seus objectius?	1,00	3,00		Millores intrínseques; Proj08; Proj09
5.3	Rols i Responsabilitats	**3,00**	**3,00**		
5.3.1	S'han assignat les responsabilitats i les autoritats sobre la Seguretat de la Informació?	3,00	3,00		Millores intrínseques; Proj08; Proj09
5.3.2	S'han comunicat convenientment les responsabilitats i les autoritats per a la Seguretat de la Informació?	3,00	3,00		Millores intrínseques; Proj08; Proj09
6	Planificació	**1,60**	**3,00**	3	
6.1	Tractament de Riscos i Oportunitats	**1,20**	**3,00**		
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?	2,00	3,00		Millores intrínseques
6.1.2	S'identifiquen i analitzen els riscos mitjançant un mètode d'avaluació i d'acceptació de riscos?	1,00	3,00		Millores intrínseques
6.1.3	S´ha definit un procés de tractament de riscos?	1,00	3,00		Millores intrínseques
6.1.4	S'han establert criteris per elaborar una declaració d'aplicabilitat?	1,00	3,00		Millores intrínseques
6.1.5	Es manté informació documentada dels punts anteriors?	1,00	3,00		Millores intrínseques
6.2	Planificació per aconseguir objectius	**2,00**	**3,00**		
6.2.1	S'han establert objectius de la Seguretat de la Informació mesurables i d'acord amb els objectius del negoci?	2,00	3,00		Millores intrínseques
6.2.2	Els objectius de la Seguretat de la Informació estan planificats mitjançant?-Assignació de responsabilitats -Cronograma d'execució temporal -Mètode d'avaluació	2,00	3,00		Millores intrínseques
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?	2,00	3,00		Millores intrínseques
7	Suport	**2,73**	**3,73**	4	
7.1	Recursos	**2,00**	**3,00**		
7.1.1	S'identifiquen i assignen els recursos necessaris per a l'SGSI?	2,00	3,00		Millores intrínseques
7.2	Competència	**3,00**	**4,00**		
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?	3,00	4,00		Millores intrínseques; Proj02
7.2.2	Es manté informació actualitzada sobre la competència del personal?	3,00	4,00		Millores intrínseques; Proj02
7.3	Conscienciació	**3,00**	**4,00**		
7.3.1	El personal està involucrat i és conscient del seu paper a la Seguretat de la Informació?	3,00	4,00		Millores intrínseques; Proj01
7.3.2	Hi ha consciència dels danys que es poden produir de no seguir les pautes de la Seguretat de la Informació?	3,00	4,00		Millores intrínseques; Proj01
7.4	Comunicació	**3,00**	**4,00**		
7.4.1	Es comunica la política de la Seguretat de la Informació amb les responsabilitats de cadascú?	3,00	4,00		Millores intrínseques; Proj01; Proj02

7.4.2	Hi ha un procés per comunicar les deficiències o males pràctiques en la seguretat de la informació?	3,00	4,00		Millores intrínseques; Proj01; Proj02
7.5	Informació Documentada	**2,67**	**3,67**		
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.)	2,00	4,00		Millores intrínseques
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	3,00	4,00		Millores intrínseques
7.5.3	Es controlen els documents d'origen extern?	3,00	3,00		Millores intrínseques
8	Operació	**1,33**	**3,17**	3	
8.1	Control Operacional	**2,00**	**3,50**		
8.1.1	Els processos de seguretat de la informació estan documentats per controlar que es realitzen segons el planificat?	2,00	4,00		Millores intrínseques
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?	2,00	4,00		Millores intrínseques
8.1.3	S'estableixen mesures i plans per mitigar els riscos a la Seguretat de la Informació davant de canvis realitzats?	2,00	3,00		Millores intrínseques
8.1.4	S'identifiquen i es controlen els processos externalitats quant als riscos per a la Seguretat de la Informació?	2,00	3,00		Millores intrínseques
8.2	Anàlisi de riscos de la Seguretat de la Informació	**1,00**	**3,00**		
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	1,00	3,00		Millores intrínseques
8.3	Tractament de riscos de la Seguretat de la Informació	**1,00**	**3,00**		
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	1,00	3,00		Millores intrínseques
8.3.2	S'identifiquen tots els controls necessaris per mitigar el risc justificant-ne l'aplicació?	1,00	3,00		Millores intrínseques
8.3.3	Es documenta el nivell d'aplicació de tots els controls que cal aplicar?	1,00	3,00		Millores intrínseques
9	Avaluació de l'exercici	**2,78**	**3,61**	4	
9.1	Seguiment i mesurament	**3,00**	**3,50**		
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?	3,00	3,00		Millores intrínseques; Proj09

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?	3,00	4,00		Millores intrínseques; Proj09
9.2	Auditories Internes	**2,33**	**3,33**		
9.2.1	S'ha establert una programació d'auditories internes i assignat responsables?	3,00	4,00		Millores intrínseques; Proj09
9.2.2	L'abast i els requisits s'han definit per a l'informe d'auditoria?	2,00	3,00		Millores intrínseques; Proj09
9.2.3	Es consideren accions correctives i propostes de canvi als informes d'auditoria?	2,00	3,00		Millores intrínseques; Proj09
9.3	Informe de Revisió per la Direcció	**3,00**	**4,00**		
9.3.1	Hi ha una programació per als informes de la direcció i hi ha constància de la seva realització periòdica?	3,00	4,00		Millores intrínseques; Proj09
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?	3,00	4,00		Millores intrínseques; Proj09
10	Millora	**2,25**	**3,50**	4	
10.1	No Conformitats i accions correctives	**2,50**	**4,00**		
10.1.1	Hi ha un procediment documentat per identificar i registrar les no-conformitats i el seu tractament?	3,00	4,00		Millores intrínseques; Proj08; Proj09
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?	2,00	4,00		Millores intrínseques; Proj08; Proj09
10.2	Millora continua	**2,00**	**3,00**		
10.2.1	Hi ha un procés per garantir la millora contínua de l'SGSI identificant les oportunitats de millora?	2,00	3,00		Millores intrínseques; Proj08; Proj09

Taula 84. Valoració maduresa assolida de la norma

Secció	Requeriment	Aplica	Nivell de compliment	Nivell assolit	Nivell objectiu	Indicador	Projecte	Anàlisi
A.5	Polítiques de seguretat de la informació		**2,00**	**3,50**	**4**			
A.5.1	Directrius de gestió de la seguretat de la informació		**2,00**	**3,50**				
A.5.1.1	Polítiques per a la seguretat de la informació	SI	2,00	4,00		Ind01	Millores intrínseques; Proj08; Proj09	S'ha definit una política de seguretat, associada a aquest treball. Així com una revisió i actualització de tots els procediments existents. També s'han creat procediments nous

A.5.1.2	Revisió de les polítiques per a la seguretat de la informació	SI	2,00	3,00		Ind01	Millores intrínseques; Proj08; Proj09	Amb la creació de la política de seguretat i la revisió dels procediments i la creació dels nous s'ha definit una política de revisió, però encara no es pot qualificar aquesta revisió. En auditories posteriors el nivell de maduresa podrà millorar
A.6	Organització de la Seguretat de la informació		**1,80**	**4,00**	**4**			
A.6.1	Organització interna		**2,60**	**4,00**				**Les formacions especifiques a administradors ajudarà a fer més efectives les responsabilitats i definir els rols d'una forma més eficient**
A.6.1.1	Rols i responsabilitats en seguretat de la informació.	SI	3,00	4,00		Ind02	Millores intrínseques; Proj03	Amb la implementació del SGSI s'han definit el rols i les responsabilitat dins l'organització.
A.6.1.2	Segregació de tasques	SI	3,00	4,00		Ind02	Millores intrínseques; Proj03	La Segregació de tasques també queden definides dins els rols i les responsabilitat.
A.6.1.3	Contacte amb les autoritats	SI	3,00	4,00		Ind02	Millores intrínseques; Proj03; Proj08_9	S'ha revisat i actualitzat el procediment sobre notificació de bretxes de seguretat;
A.6.1.4	Contacte amb grups d' interès especial	SI	2,00	4,00		Ind02	Millores intrínseques; Proj03; Proj09_4	s'ha creat un procediment pel contacte amb els grups especials
A.6.1.5	Seguretat de la informació en la gestió de projectes	SI	2,00	4,00		Ind03	Millores intrínseques; Proj03; Proj09_5	S'ha creat un procediment sobre la gestió de projectes
A.6.2	Els dispositius mòbils i el teletreball		**1,00**	**4,00**				
A.6.2.1	Política de dispositius mòbils	SI	1,00	5,00		Ind01	Millores intrínseques; Proj07	La implementació d'un MDM optimitza la política i la gestió de dispositius mòbils
A.6.2.2	Teletreball	SI	1,00	3,00		Ind01, Ind02	Millores intrínseques; Proj08_10	S'ha revisat i actualitzat el procediment de Teletreball però no s'ha fet cap actuació més en aquest punt.
A.7	Seguretat relativa als recursos humans		**1,75**	**3,75**	**3**			

A.7.1	Abans de l' ocupació		**1,50**	**3,50**				**El projecte per la millora dels procediments per la contractació de personal millora tots els aspectes d'aquests controls, no obstant no s'ha pogut comprovar la millora en la investigació d'antecedents. L'actualització i millora dels acords de confidencialitat també provoquen una millora en els controls.**
A.7.1.1	Investigació d' antecedents	SI	2,00	3,00		Ind04	Proj08_15; Proj11	Igual que A.7.1
A.7.1.2	Termes i condicions de l' ocupació	SI	1,00	4,00		Ind04	Proj08_15; Proj11	Igual que A.7.1
A.7.2	Durant l' ocupació		**1,00**	**3,33**				**Juntament amb l'explicació de 7.1 el procediment de l'exercici de dret millora substancialment aquest punt**
A.7.2.1	Responsabilitats de gestió	SI	1,00	4,00		Ind04	Proj08_8; Proj08_15; Proj11	Igual que A.7.2
A.7.2.2	Conscienciació, educació i capacitació en seguretat de la informació	SI	1,00	3,00		Ind05	Proj01; Proj02; Proj08_8;Proj08_15; Proj11	el pla de formacions ajuda a millorar aquest punt però no se n'ha pogut comprovar l'efectivitat
A.7.2.3	Procés disciplinari.	SI	1,00	3,00		Ind04	Proj08_8; Proj08_15; Proj11	Igual que A.7.2
A.7.3	Finalització de l' ocupació o canvi de lloc de treball		**2,00**	**4,00**				
A.7.3.1	Responsabilitat davant la finalització o canvi	SI	2,00	4,00		Ind04	Proj08_15; Proj11	Igual que A.7.1
A.8	Gestió d'actius		**2,11**	**4,00**	**4**			S'ha creat un procediment nou per la gestió dels actius on es tenen en compte tots els controls d'aquesta àrea.
A.8.1	Responsabilitat sobre els actius		**2,00**	**4,00**				
A.8.1.1	Inventari d' actius	SI	2,00	4,00		Ind06	Proj10	Igual que A.8
A.8.1.2	Propietat dels actius	SI	2,00	4,00		Ind06	Proj10	Igual que A.8
A.8.1.3	Ús acceptable dels actius	SI	2,00	4,00		Ind07	Proj08_3; Proj10	Juntament amb el nou procediment derivat del projecte 10, també s'ha revistat i actualitzat el procediment existent sobre l'ús del actius

A.8.1.4	Devolució d' actius	SI	2,00	4,00		Ind07	Proj10	Igual que A.8
A.8.2	Classificació de la informació		**1,67**	**4,00**				
A.8.2.1	Classificació de la informació	SI	1,00	4,00		Ind01	Proj10	Igual que A.8
A.8.2.2	Etiquetatge de la informació	SI	2,00	4,00		Ind08	Proj10	Igual que A.8
A.8.2.3	Manipulat de la informació.	SI	2,00	4,00		Ind08	Proj10	Igual que A.8
A.8.3	Manipulació dels suports		**2,67**	**4,00**				
A.8.3.1	Gestió de suports extraïbles.	SI	2,00	4,00		Ind07	Proj10	Igual que A.8
A.8.3.2	Eliminació de suports	SI	3,00	4,00		Ind07	Proj10	Igual que A.8
A.8.3.3	Suports físics en trànsit	SI	3,00	4,00		Ind07	Proj10	Igual que A.8
A.9	Control d'accés		**2,94**	**3,83**	**4**			**S'han revisat i millorat els controls d'accessos a àrees restringides. La revisió i actualització de la normativa de protecció de dades, els procediments de llocs de treball net i la guia per administradors locals recullen totes les necessitats especificades als controls**
A.9.1	Requisits de negoci per al control d' accés		**3,00**	**3,50**				
A.9.1.1	Polítiques de control d' accés	SI	3,00	3,00		Ind01	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.1.2	Accés a les xarxes i als serveis de xarxa	SI	3,00	4,00		Ind09	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.2	Gestió d' accés d' usuari		**2,83**	**4,00**				
A.9.2.1	Registre i baixa d' usuari	SI	2,00	4,00		Ind10	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.2.2	Provisió d' accés d' usuari	SI	3,00	4,00		Ind10	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.2.3	Gestió de privilegis d' accés	SI	3,00	4,00		Ind10	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.2.4	Gestió de la informació secreta d' autenticació dels usuaris	SI	3,00	4,00		Ind11	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.2.5	Revisió dels drets d' accés d' usuari	SI	3,00	4,00		Ind11	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9

A.9.2.6	Retirada o reassignació dels drets d' accés	SI	3,00	4,00		Ind10	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.3	Responsabilitat de l' usuari		**3,00**	**4,00**				
A.9.3.1	Ús de la informació secreta d' autenticació	SI	3,00	4,00		Ind11	Proj06; Proj08_1, Proj08_2, Proj08_6, Proj08_15	Igual que A.9
A.9.4	Control d' accés a sistemes i aplicacions		**2,80**	**3,60**				
A.9.4.1	Restricció de l'accés a la informació	SI	3,00	4,00		Ind09	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.4.2	Procediments segurs d' inici de sessió	SI	3,00	4,00		Ind10	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.4.3	Sistemes de gestió de contrasenyes	SI	3,00	4,00		Ind11	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.4.4	Ús d' utilitats amb privilegis del sistema.	SI	3,00	3,00		Ind10	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.9.4.5	Control d' accés al codi font dels programes	SI	2,00	3,00		Ind09	Proj06; Proj08_1, Proj08_2, Proj08_15	Igual que A.9
A.10	Criptografia		**2,00**	**3,00**	**3**			
A.10.1	Controls criptogràfics		**2,00**	**3,00**				
A.10.1.1	Polítiques d' ús dels controls criptogràfics	SI	3,00	3,00		Ind01	Proj08_11	Es recull l'ús de certificats en la guia de bones pràctiques
A.10.1.2	Gestió de Claus	SI	1,00	3,00		Ind02	Proj09_2	S'ha creat un procediment sobre la gestió de les claus criptogràfiques
A.11	Seguretat física i de l'entorn		**2,72**	**3,47**	**4**			
A.11.1	Àrees segures		**3,00**	**3,50**				
A.11.1.1	Perímetre de seguretat física	SI	3,00	4,00		Ind02, Ind12	Proj06; Proj09_1	Es revisa i s'executen millores en el control d'accés a àrees segures i es revisen tots les infraestructures de xarxa i accessos de les oficines i es fan les actuacions necessàries per assegurar-les
A.11.1.2	Controls físics d' entrada	SI	3,00	4,00		Ind12	Proj06; Proj09_1	En el nou protocol definit es recull els procediments d'assignació, modificació i revocació de permisos i es milloren els accessos a aquestes zones

A.11.1.3	Seguretat d' oficines, despatxos i recursos	SI	3,00	3,00		Ind12	Proj06; Proj08_11, Proj08_15 ; Proj09_1	Es recullen conceptes sobre seguretat d'oficines i despatxos en projectes com la guia de bones pràctiques i la guia d'administradors territorials.
A.11.1.4	Protecció contra les amenaces externes i ambientals	SI	3,00	4,00		Ind12	Proj06; Proj09_1	Igual que A.11.1.1
A.11.1.5	El treball en àrees segures	SI	3,00	3,00		Ind12	Proj06; Proj09_1	Igual que A.11.1.1
A.11.1.6	Àrees de càrrega i descàrrega	SI	3,00	3,00		Ind12	Proj06; Proj09_1	Igual que A.11.1.3
A.11.2	Seguretat dels equips		**2,44**	**3,44**				
A.11.2.1	Emplaçament i protecció d' equips	SI	2,00	4,00		Ind13	Proj06; Proj08_2, Proj08_11, Proj08_15; Proj09_1	Aquests procediments queden recollits plenament en el procediments revisats i actualitzats
A.11.2.2	Instal·lacions de subministrament	SI	3,00	3,00		Ind13	Proj06; Proj08_11, Proj08_15; Proj09_1	Igual que A.11.1.3
A.11.2.3	Seguretat del cablejat	SI	2,00	3,00		Ind13	Proj06; Proj08_11, Proj08_15; Proj09_1	Igual que A.11.1.3
A.11.2.4	Manteniment dels equips	SI	2,00	4,00		Ind14	Proj06; Proj08_2, Proj08_11, Proj08_15; Proj09_1	Igual que A.11.2.1
A.11.2.5	Retirada de materials de l' empresa	NO	3,00	3,00				
A.11.2.6	Seguretat dels equips fora de les instal·lacions	NO	2,00	3,00				
A.11.2.7	Reutilització o eliminació segura d' equips	SI	3,00	4,00		Ind07, Ind14	Proj08_2, Proj08_11, Proj08_15; Proj10	Igual que A.11.2.1
A.11.2.8	Equip d' usuari desatès	SI	3,00	4,00		Ind01	Proj08_2, Proj08_11, Proj08_15	Igual que A.11.2.1
A.11.2.9	Política de lloc de treball ordenat i pantalla neta	SI	2,00	3,00		Ind01	Proj01; Proj08_2, Proj08_11, Proj08_15; Proj09_1	Igual que el control A.11.2.1 juntament amb les campanyes de conscienciació queden recollides els requeriments d'aquest control
A.12	Seguretat de les operacions		**2,57**	**3,82**	**4**			
A.12.1	Requisits de negoci per al control d' accés		**2,50**	**3,75**				El nou procediment sobre la gestió de projectes i procediments com la guia per administradors locals recullen aquests requisits

A.12.1.1	Documentació de procediments operacionals	SI	3,00	4,00		Ind01	Proj03; Proj08_15; Proj09_1, Proj09_5	Igual que A.12.1
A.12.1.2	Gestió de canvis	SI	2,00	4,00		Ind15	Proj03; Proj08_15; Proj09_1, Proj09_5	Igual que A.12.1
A.12.1.3	Gestió de capacitats	SI	2,00	4,00		Ind15	Proj03; Proj08_15; Proj09_1, Proj09_5	Igual que A.12.1
A.12.1.4	Separació dels recursos de desenvolupament, prova i operació	SI	3,00	3,00		Ind16	Proj03; Proj08_14, Proj08_15; Proj09_1, Proj09_5	En tots els projectes indicats es recullen conceptes sobre la separació entre entorn de proves i d'operacions
A.12.2	Protecció contra el programari maliciós (malware		**2,00**	**5,00**				
A.12.2.1	Controls contra el codi maliciós	SI	2,00	5,00		Ind17	Proj03; Proj04; Proj08_15; Proj09_1, Proj09_5	les bones pràctiques i la implementació del nou sistema recollit al projecte 4 optimitzen aquest control
A.12.3	Còpies de seguretat		**3,00**	**4,00**				
A.12.3.1	Còpies de seguretat de la informació	SI	3,00	4,00		Ind01	Proj03; Proj05; Proj08_15; Proj09_1, Proj09_5	El nou procediment de copies de seguretat millora substancialment l'anterior i compleix perfectament
A.12.4	Registres i supervisió		**3,00**	**3,50**				
A.12.4.1	Registres d' esdeveniments.	SI	3,00	4,00		Ind18	Proj03; Proj08_13, Proj08_14; Proj08_15, Proj08_16; Proj09_1, Proj09_5	Molts procediments definits milloren el compliment d'aquest control, sobretot el procediment sobre la gestió de Logs
A.12.4.2	Protecció de la informació del registre	SI	3,00	4,00		Ind18	Proj03; Proj05; Proj08_15, Proj08_16; Proj09_1, Proj09_5	El procediment sobre la gestió de Logs i les copies de seguretat donen compliment a aquest control
A.12.4.3	Registres d' administració i operació	SI	3,00	3,00		Ind18	Proj03; Proj08_15; Proj09_1, Proj09_5	No es troben canvis substancials en els procediments respecte aquest control tot i complir i no detectar-hi deficiències
A.12.4.4	Sincronització del rellotge	SI	3,00	3,00		Ind18	Proj03; Proj08_15; Proj09_1, Proj09_5	No es troben canvis substancials en els procediments respecte aquest control tot i complir i no detectar-hi deficiències
A.12.5	Control del programari en explotació		**3,00**	**4,00**				

A.12.5.1	Instal·lació del programari en explotació	SI	3,00	4,00		Ind16	Proj03; Proj08_15; Proj09_1, Proj09_5	La guia per administradors locals, i el procediment de gestió de projectes, juntament amb una formació adequada dels administradors obtenim uns bons nivells en el compliment d'aquests controls
A.12.6	Gestió de la vulnerabilitat tècnica		**2,50**	**3,50**				
A.12.6.1	Gestió de les vulnerabilitats tècniques	SI	3,00	4,00		Ind17	Proj03; Proj08_09, Proj08_15; Proj09_1, Proj09_5	La guia per administradors locals, i el procediment de gestió de projectes, juntament amb una formació adequada dels administradors obtenim uns bons nivells en el compliment d'aquests controls
A.12.6.2	Restricció en la instal·lació del programari	SI	2,00	3,00		Ind01	Proj03; Proj08_15; Proj09_1, Proj09_5	EL procediment de notificació de bretes, la guia per administradors locals, i el procediment de gestió de projectes, juntament amb una formació adequada dels administradors obtenim uns bons nivells en el compliment d'aquests controls
A.12.7	Consideracions sobre l' auditoria de sistemes d' informació		**2,00**	**3,00**				
A.12.7.1	Controls d' auditoria de sistemes d' informació	SI	2,00	3,00		Ind18	Proj03; Proj08_15; Proj09_1, Proj09_5	La guia per administradors locals, i el procediment de gestió de projectes, juntament amb una formació adequada dels administradors obtenim uns bons nivells en el compliment d'aquests controls
A.13	Seguretat de les comunicacions		**3,17**	**3,50**	**4**			
A.13.1	Gestió de la seguretat de les xarxes		**3,33**	**3,00**				No s'ha realitzat cap projecte enfocat en aquests controls, existien ja bones pràctiques i compliments en aquests. Si s'està formant als administradors en aquests aspectes, juntament amb tots els procediments existents existirà una millora en següents auditories
A.13.1.1	Controls de xarxa	SI	3,00	3,00		Ind09	Proj03	Igual que A.13.1.1
A.13.1.2	Seguretat dels serveis de xarxa	SI	3,00	3,00		Ind09	Proj03	Igual que A.13.1.1
A.13.1.3	Segregació en xarxes	SI	4,00	4,00		Ind09	Proj03	Igual que A.13.1.1

A.13.2	Intercanvi d' informació.		**3,00**	**4,00**				
A.13.2.1	Polítiques i procediments d' intercanvi d' informació	SI	2,00	4,00		Ind01	Proj03; Proj08_5, Proj08_12, Proj08_17	El procediment específic sobre procediments d'intercanvi d'informació més altres procediments donen un bon compliment a aquest control
A.13.2.2	Acords d' intercanvi d' informació	SI	3,00	4,00		Ind01	Proj03; Proj08_5, Proj08_12, Proj08_17	Igual que A.13.2.1
A.13.2.3	Missatgeria electrònica	SI	4,00	4,00		Ind17	Proj03; Proj08_4, Proj08_5, Proj08_6, Proj08_12, Proj08_17	ja hi havia un bon compliment, es millora encara una mica mes amb la revisió de la guia d'ús del correu electrònic i la guia d'orientació sobre missatgeria i xarxes socials
A.13.2.4	Acords de confidencialitat o no revelació.	SI	3,00	4,00		Ind01	Proj03; Proj08_5, Proj08_12, Proj08_17	El procediment sobre acords de confidencialitat donen bon compliment
A.14	Adquisició, desenvolupament i manteniment dels sistemes d'informació		**2,78**	**3,67**	**4**			
A.14.1	Requisits de seguretat en els sistemes d' informació		**2,67**	**3,33**				
A.14.1.1	Anàlisi de requisits i especificacions de seguretat de la informació	SI	2,00	4,00		Ind19	Proj03; Proj09_6	Existeix un procediment específic per l'adquisició de nous component.
A.14.1.2	Assegurar els serveis d' aplicacions en xarxes públiques	SI	3,00	3,00		Ind17	Proj03	No s'ha creat cap projecte per la millora d'aquest punt, tot i que ja existeix un bon compliment i bona pràctica en aquest control
A.14.1.3	Protecció de les transaccions de serveis d' aplicacions	SI	3,00	3,00		Ind17	Proj03	Igual que A.14.1.2
A.14.2	Seguretat en el desenvolupament i en els processos de suport		**2,67**	**3,67**				Els procediment de desenvolupament segur, la guia per administradors locals recullen, guien i donen compliment als controls
A.14.2.1	Política de desenvolupament segur	SI	2,00	4,00		Ind01	Proj03; Proj08_13, Proj08_15	Igual que A.14.2.1
A.14.2.2	Procediment de control de canvis en sistemes.	SI	2,00	4,00		Ind15	Proj03; Proj08_13, Proj08_15	Igual que A.14.2.1
A.14.2.3	Revisió tècnica de les aplicacions després d' efectuar canvis en el sistema operatiu.	SI	2,00	4,00		Ind15	Proj03; Proj08_13, Proj08_15	Igual que A.14.2.1
A.14.2.4	Restriccions als canvis en els paquets de programari	SI	3,00	4,00		Ind16	Proj03; Proj08_13, Proj08_15	Igual que A.14.2.1

A.14.2.5	Principis d' enginyeria de sistemes segurs	SI	3,00	4,00		Ind09, Ind15, Ind16	Proj03; Proj08_13, Proj08_15	Igual que A.14.2.1
A.14.2.6	Entorn de desenvolupament segur	SI	3,00	4,00		Ind16	Proj03; Proj08_13, Proj08_15	Igual que A.14.2.1
A.14.2.7	Externalització del desenvolupament de programari.	NO	3,00	3,00				
A.14.2.8	Proves funcionals de seguretat de sistemes	SI	3,00	3,00		Ind20	Proj03; Proj08_13, Proj08_15	Igual que A.14.2.1
A.14.2.9	Proves d' acceptació de sistemes	SI	3,00	3,00		Ind20	Proj03; Proj08_13, Proj08_15	Igual que A.14.2.1
A.14.3	Dades de prova		**3,00**	**4,00**				
A.14.3.1	Protecció de les dades de prova.	SI	3,00	4,00		Ind20	Proj03; Proj05	S'han inclòs en les copies de seguretat
A.15	Relació amb proveïdors		**3,00**	**3,83**	**4**			El procediment sobre contractació de proveïdors recull tots els controls d'aquest domini
A.15.1	Seguretat en les relacions amb proveïdors		**3,00**	**3,67**				
A.15.1.1	Política de seguretat de la informació en les relacions amb els proveïdors	SI	3,00	4,00		Ind01	Proj08_17	Igual que A.15
A.15.1.2	Requisits de seguretat en contractes amb tercers	SI	3,00	4,00		Ind21	Proj08_17	Igual que A.15
A.15.1.3	Cadena de subministrament de tecnologia de la informació i de les comunicacions	SI	3,00	3,00		Ind21	Proj08_17	Igual que A.15
A.15.2	Gestió de la provisió de serveis del proveïdor		**3,00**	**4,00**				
A.15.2.1	Control i revisió de la provisió de serveis del proveïdor	SI	3,00	4,00		Ind21	Proj08_17	Igual que A.15
A.15.2.2	Gestió de canvis en la provisió del servei del proveïdor	SI	3,00	4,00		Ind21	Proj08_17	Igual que A.15
A.16	Gestió d'incidents de seguretat de la informació		**2,86**	**3,57**	**4**			
A.16.1	Gestió d' incidents de seguretat de la informació i millores		**2,86**	**3,57**				L'elaboració d'aquest treball juntament amb les millores procedimentals com el procediment d'exercici de dret i la notificació de bretxes de seguretat donen compliment als controls de compliment.

A.16.1.1	Responsabilitats i procediments	SI	2,00	4,00		Ind01, Ind02	Millores intrínseques; Proj08_8	Igual que A.16.1
A.16.1.2	Notificació dels esdeveniments de seguretat de la informació.	SI	3,00	4,00		Ind01	Millores intrínseques; Proj08_8; Proj08_9	Igual que A.16.1
A.16.1.3	Notificació de punts febles de la seguretat	SI	3,00	3,00		Ind19	Millores intrínseques; Proj08_8; Proj08_9	Igual que A.16.1
A.16.1.4	Avaluació i decisió sobre els esdeveniments de seguretat d' informació	SI	3,00	4,00		Ind19	Millores intrínseques; Proj08_8	Igual que A.16.1
A.16.1.5	Resposta a incidents de seguretat de la informació.	SI	3,00	4,00		Ind19	Millores intrínseques; Proj08_8	Igual que A.16.1
A.16.1.6	Aprenentatge dels incidents de seguretat de la informació	SI	3,00	3,00		Ind19	Millores intrínseques; Proj08_8	Igual que A.16.1
A.16.1.7	Recopilació d' evidències	SI	3,00	3,00		Ind19	Millores intrínseques; Proj08_8	Igual que A.16.1
A.17	Aspectes de seguretat de la informació per la gestió de la continuïtat del negoci		**3,17**	**3,67**	**4**			
A.17.1	Continuïtat de la seguretat de la informació		**2,33**	**3,33**				
A.17.1.1	Planificació de la continuïtat de la seguretat de la informació	SI	1,00	4,00		Ind22	Proj09_3	Queda recollit amb el desenvolupament del pla de continuïtat de negoci elaborat
A.17.1.2	Implementar la continuïtat de la seguretat de la informació	SI	3,00	3,00		Ind22	Proj09_3	No s'ha pogut avaluar
A.17.1.3	Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	SI	3,00	3,00		Ind18	Proj09_3	No s'ha pogut avaluar
A.17.2	Redundàncies		**4,00**	**4,00**				
A.17.2.1	Disponibilitat dels recursos de tractament de la informació	SI	4,00	4,00		Ind22		Existeixen les redundàncies necessàries
A.18	Compliment		**2,30**	**3,90**	**4**			**L'elaboració d'aquest treball juntament amb les millores procedimentals com la guia de protecció de dades i els procediment d'exercici de dret donen compliment als controls de compliment.**
A.18.1	Compliment dels requisits legals i contractuals		**2,60**	**3,80**				
A.18.1.1	Identificació de la legislació aplicable i dels requisits contractuals	SI	1,00	4,00		Ind23	Millores intrínseques; Proj08_7, Proj08_8	Igual que A.18

A.18.1.2	Drets de Propietat Intel·lectual (DPI).	SI	2,00	4,00		Ind23	Millores intrínseques; Proj08_7, Proj08_8	Igual que A.18
A.18.1.3	Protecció dels registres de l' organització	SI	3,00	4,00		Ind23	Millores intrínseques; Proj08_7, Proj08_8	Igual que A.18
A.18.1.4	Protecció i privacitat de la informació de caràcter personal.	SI	4,00	4,00		Ind23	Millores intrínseques; Proj08_7, Proj08_8	Igual que A.18
A.18.1.5	Regulació dels controls criptogràfics	SI	3,00	3,00		Ind23	Millores intrínseques; Proj08_7, Proj08_8	Igual que A.18
A.18.2	Revisió independent de la seguretat de la informació		**2,00**	**4,00**				
A.18.2.1	Revisió independent de la seguretat de la informació	SI	2,00	4,00		Ind18	Millores intrínseques; Proj08_7, Proj08_8	Igual que A.18
A.18.2.2	Compliment de les polítiques i normes de seguretat	SI	2,00	4,00		Ind23	Millores intrínseques; Proj08_7, Proj08_8	Igual que A.18
A.18.2.3	Comprovació del compliment tècnic.	SI	2,00	4,00		Ind18	Millores intrínseques; Proj08_7, Proj08_8	Igual que A.18

Taula 85. Valoració maduresa assolit pels controls

18. Annex 9 Auditoria de Compliment

<table>
<tr><th colspan="3">Organització</th><td rowspan="4">LOGO</td></tr>
<tr><th colspan="2">Nom del document</th><th>Codi de document</th></tr>
<tr><td colspan="2">Procediment d'auditories internes</td><td>PAI-SI.ORG01</td></tr>
<tr><th>Versió</th><th>Data</th><th>Autor</th></tr>
<tr><td>1.0</td><td>23/12/2022</td><td>Marc Vilalta Parra</td><td></td></tr>
<tr><td colspan="4">Abast Aquesta auditoria es centre en la implementació de la norma ISO 27001 en tots els àmbits en la que la seguretat de la informació té incidència dins l'Organització</td></tr>
<tr><td colspan="4">Equip Auditor L'equip auditor està format per l'autor d'aquest informe juntament amb el responsable de seguretat i del departament de SI, amb col·laboració d'una empresa auditora externa.</td></tr>
<tr><td colspan="4">Objectiu Valorar si el procés d'implementació de la norma ISO 27001 realitzat s'ha fet correctament i s'han assolit els objectius plantejats per l'organització al inici del procés.</td></tr>
<tr><td colspan="4">Tasques realitzades s'ha realitzat un anàlisi dels controls de la ISO 27002, annex 8, per valorar el nivell de maduresa actual, s'han valorat i analitzat els projectes plantejats i les tasques realitzades, així com els indicadors.</td></tr>
<tr><td colspan="4">Resultats s'han detectat els següents punts que s'haurien de tractar
No conformitats menors
A.8.3.2 Eliminació de suports
A.9.1.1 Polítiques de control d' accés
A.10.1.1 Polítiques d' ús dels controls criptogràfics
A.11.2.9 Política de lloc de treball ordenat i pantalla neta
A.14.2.8 Proves funcionals de seguretat de sistemes
A.14.2.9 Proves d' acceptació de sistemes
Observacions
A.8.2.2 Etiquetatge de la informació
A.10.1.2 Gestió de Claus
A.11.1.3 Seguretat d' oficines, despatxos i recursos
A.11.1.6 Àrees de càrrega i descàrrega
A.12.1.4 Separació dels recursos de desenvolupament, prova i operació
A.16.1.3 Notificació de punts febles de la seguretat
Aquestes es troben desenvolupades a la Taula 53 del present treball</td></tr>
<tr><td colspan="4">Recomanacions Treballar en les no conformitats menors de manera immediata i seguir treballant en la línia que s'ha traçat seguint el pla de millora continuada, que permetrà aconseguir el nivell de maduresa objectiu en tots els controls de la ISO 27002 en futures auditories.</td></tr>
</table>