Sistema de Gestió de la Seguretat de la Informació seguint la norma ISO 27001 – ISO 27002 per a l'empresa INGENSA, S.L.

Nom Estudiant: Jordi Sánchez Celma

Programa: Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)
Àrea: Sistemes de Gestió de la Seguretat de la Informació

Consultor: Arsenio Tortajada Gallego
Professor responsable de l'assignatura: Carles Garrigues Olivella
Centre: Universitat Oberta de Catalunya

Data Lliurament: 06/06/2016

FITXA DEL TREBALL FINAL

Títol del treball:	*Sistema de Gestió de la Seguretat de la Informació seguint la norma ISO 27001 – ISO 27002 per a l'empresa INGENSA, S.L.*
Nom de l'autor:	*Jordi Sánchez Celma*
Nom del consultor/a:	*Arsenio Tortajada Gallego*
Nom del PRA:	*Carles Garrigues Olivella*
Data de lliurament (mm/aaaa):	*06/2016*
Titulació o programa:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)
Àrea del Treball Final:	*Sistemes de Gestió de la Seguretat de la Informació*
Idioma del treball:	*Català*
Paraules clau	*Actiu* *Informació* *Seguretat*

Resum del Treball (màxim 250 paraules):

La finalitat d'aquest TFM ha estat avaluar l'estat de seguretat de la informació actual de l'empresa INGENSA, S.L., crear un SGSI, aplicar-lo i realitzar les auditories necessàries per a verificar el compliment de la norma ISO/IEC 27001 i, en cas necessari, permetre a la companyia obtindre la certificació.

El TFM es desenvolupa sobre l'empresa INGENSA, S.L., es tracta d'una empresa multinacional d'enginyeria, consultoria i tecnologies de la informació, afectant únicament a la seva seu central a Madrid.

S'ha utilitzat el model de maduresa (CMM) per als 114 controls de la norma ISO/IEC 27002:2013 i s'ha avaluat el seu compliment abans i després d'aplicar el SGSI. S'ha realitzat un inventari d'actius, per poder realitzar posteriorment un anàlisi de riscos segons la metodologia MAGERIT v.3 i posteriorment s'han realitzat propostes de projectes per millorar la segureta de la informació de la companyia. Finalment es realitza una auditoria de compliment on s'avalua

l'efectivitat del SGSI.

Amb l'aplicació del SGSI a la companyia, s'obté una millora substancial en l'estat de maduresa i compliment de tots els controls de la norma ISO/IEC 27002:2013.

Podem concloure que l'aplicació d'un sistema SGSI és beneficiós per a la companyia, ja que augmenta la seguretat dels seus actius (informació, software, serveis...) i millora la reputació de la companyia.

Abstract (in English, 250 words or less):

The purpose of this TFM has been to evaluate the current state of information security of the company INGENSA, S.L., create an ISMS, apply it and carry out the necessary audits to verify compliance of the ISO/IEC 27001 and allow to the company obtain the certification.

The TFM is developed on the company INGENSA, S.L., it is a multinational company of engineering, consulting and information technologies, affecting only its headquarters in Madrid.

It has been used the maturity model (CMM) for 114 controls of the ISO/IEC 27002:2013 and has assessed its compliance with before and after applying the ISMS. It has carried out an inventory of assets, to be able to perform then a risk analysis according to the MAGERIT methodology v.3 and later we have been made project proposals to improve the security of the information of the company. Finally is carried out an audit of compliance where we evaluate the effectiveness of the ISMS.

With the implementation of the ISMS for the company, we get a substantial improvement in the State of maturity and compliance with all the controls of the ISO/IEC 27002:2013.

We can conclude that the application of ISMS has a beneficial effect for the company, because it increases the security of your assets (information, software, services…) and it improves the reputation of the company.

Índex

Llista de figures

Llista de taules

1. Introducció

1.1 Introducció al projecte

Amb aquest Treball Final de Màster (TFM) es pretén elaborar un Sistema de Gestió de la Seguretat de la Informació per a una empresa privada fent servir les normes ISO/IEC 27001 i ISO/IEC 27002.

S'ha d'elaborar un Pla Director de Seguretat que ens ha de servir per guiar a l'organització a la realització d'una gestió adequada de la seguretat, gràcies a aquest Pla Director de Seguretat la companyia coneixerà el seu estat actual i tindrà un mètode d'actuació tant per millorar com per a solucionar incidents i així tindrem una companyia més segura al aconseguir reduir i minimitzar els seus riscos.

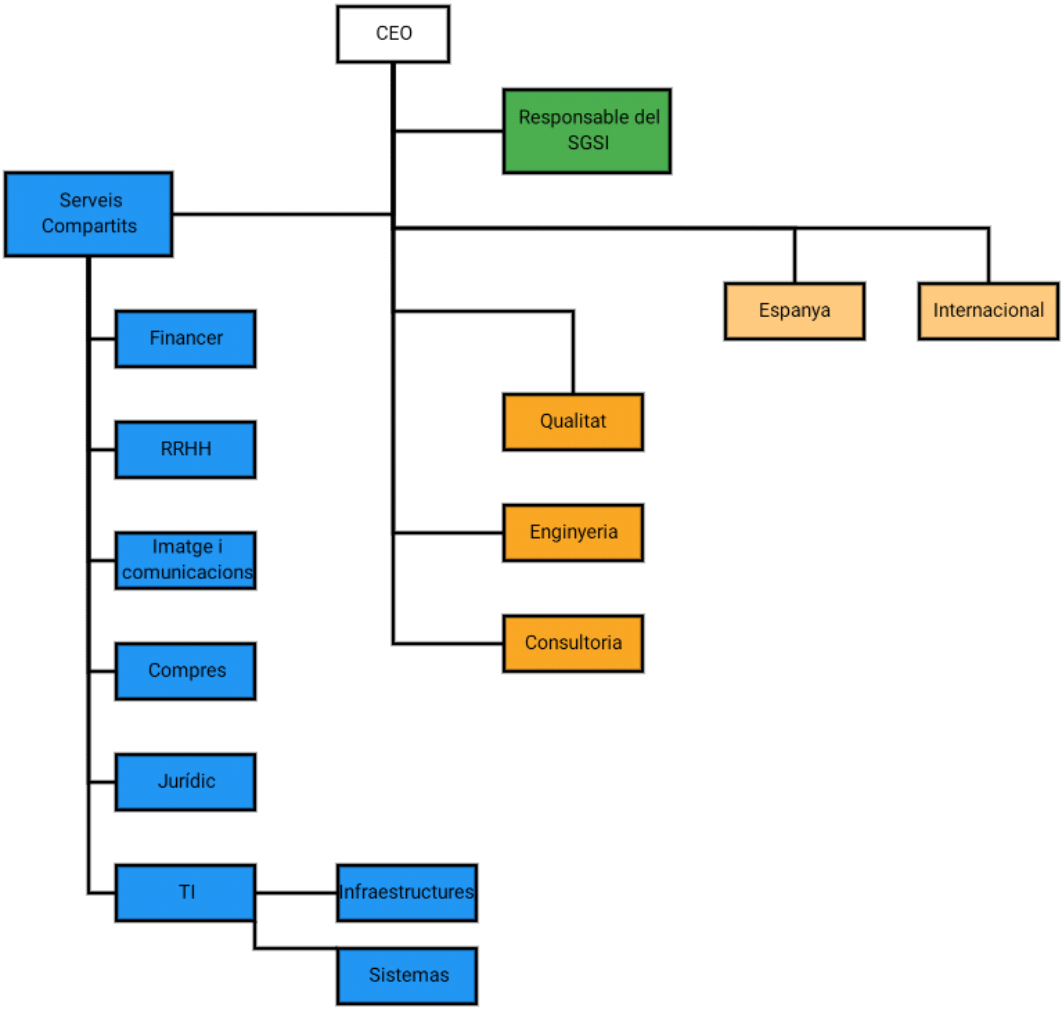
1.2 Enfocament i selecció de l'empresa objecte d'estudi

He seleccionat l'empresa INGENSA S.L., es tracta d'una companyia multinacional d'enginyeria, consultoria i tecnologies de la informació amb més de 60 anys de recorregut.

És una companyia puntera al seu sector, realitzant principalment projectes d'indole públic. Les oficines centrals del grup empresarial es troben ubicades a Madrid, on es troba el CPD principal de la companyia, encara que disposa de seus a diferents ciutats com Barcelona, Bilbao, A Coruña... i a nivell internacional, amb seus a Romania, India, Bèlgica... Disposa d'una plantilla de més de 1000 treballadors entre els diferents departaments i oficines.

Els seus sistemes d'informació estan formats per un directori actiu amb la informació replicada a les diferents seus, servei de correu electrònic, intranet corporativa, lloc web, serveis al núvol, aplicatiu CRM i ERP i connexió entre seus VPN. Així mateix, existeix la possibilitat de compartir informació entre els seus clients oferint un servei de emmagatzematge virtual.

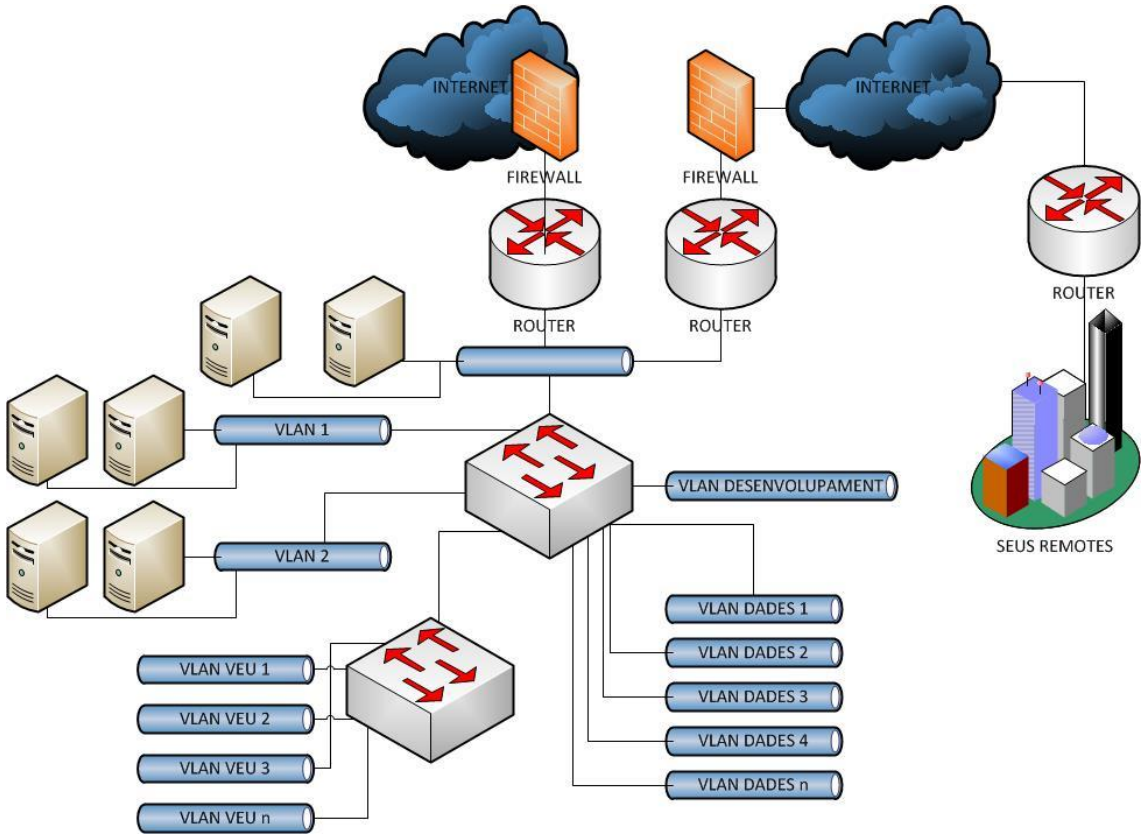
La companyia té l'organigrama organitzatiu següent:



Imatge 1: Organigrama de l'empresa INGENSA, S.L..

La companyia es troba a pràcticament totes les comunitats autònomes d'Espanya i a països de 4 dels 5 continents.

La seu central té el següent diagrama de xarxa:



Imatge 2: Diagrama de xarxa de l'empresa INGENSA, S.L.

1.3 Objectius del Pla Director de Seguretat

Gràcies al Pla Director de Seguretat, podrem indicar a la companyia quins són els projectes que haurà de realitzar per a poder garantir una correcta gestió de la seguretat de la informació. El definirem amb base a l'estratègia de negoci i les seves necessitats específiques, per tant, haurem d'identificar els processos de negoci i els seus actius.

Per a la seva realització prenem com a base la ISO/IEC 27002 i totes les normatives i estàndards aplicables que tinguin relació amb la companyia.

Realitzarem un anàlisi tècnic de vulnerabilitats mitjançant tests d'intrusió interns i externs.

Degut al gran dispersió geogràfica del treballadors, la companyia es troba en la necessitat de crear unes directrius de seguretat més exhaustives que les actuals. Per tant, els principals objectius del Pla Director de Seguretat són:

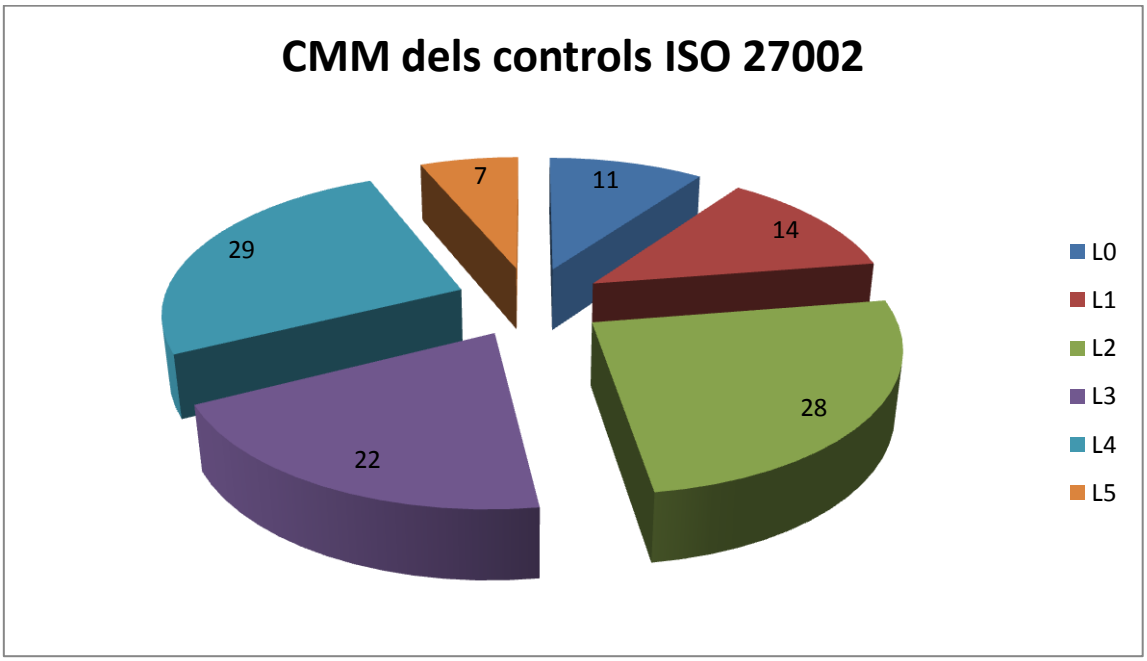
- Identificació d'actius i processos crítics.
- Garantir el compliment de la legislació que aplica a la companyia, tant en LOPD com a nivell dels projectes d'enginyeria que es realitzen.
- Sensibilitzar a l'alta direcció per aconseguir el seu recolzament.
- Assegurar les dades dels dispositius mòbils, ja que es disposa d'una gran quantitat d'ells.
- Garantir les comunicacions entre les diferents seus i la central amb un nivell de servei superior al 90%.
- Garantir la funcionalitat del servei de correu electrònic corporatiu amb un nivell de servei superior al 95%.
- Garantir la seguretat de les dades i del compliment de la normativa en quant als històrics de còpia.
- Garantir la funcionalitat dels serveis oferts als clients amb un nivell de servei superior al 99%.
- Minimitzar l'impacte front a incidents de seguretat i garantir el correcte restabliment del servei dins d'un temps estipulat.
- Analitzar els costos dels serveis de seguretat i del manteniment dels sistemes d'informació, per garantir el correcte funcionament dels controls establerts.
- Creació de la política de seguretat de la companyia.
- Conscienciació als empleats per al correcte funcionament dels controls.
- Creació d'un comitè de seguretat encarregat de la supervisió i execució dels controls.

Amb tot això la companyia tindrà una millor imatge front als clients i en cas necessari podria obtindre la certificació de seguretat.

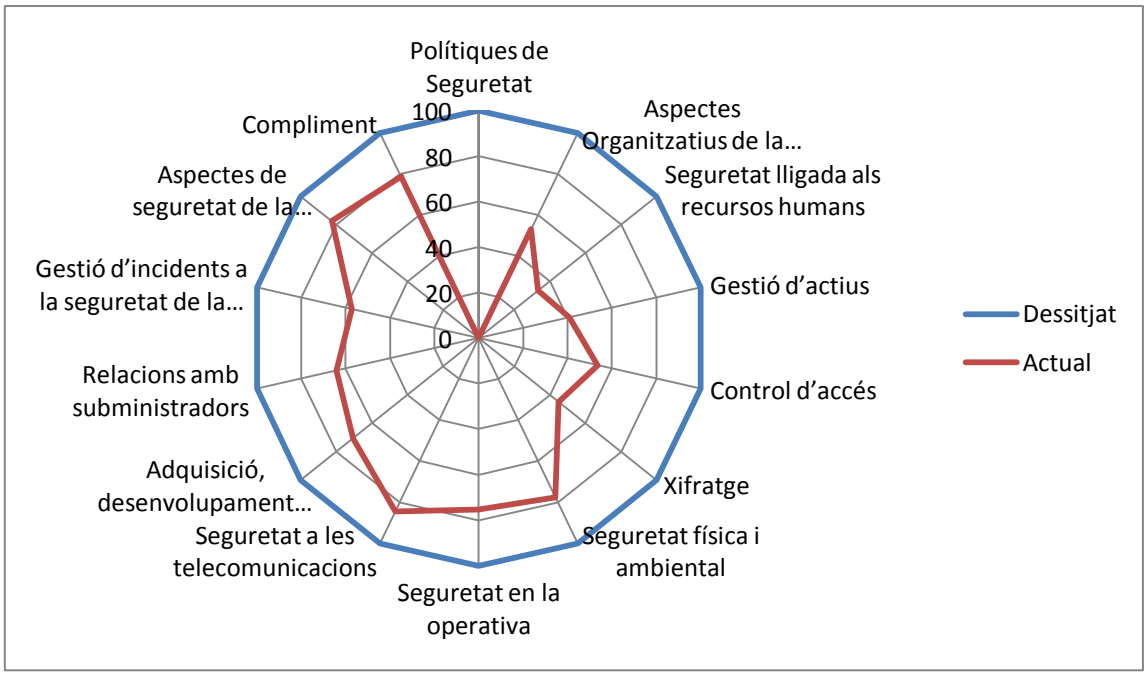
1.4 Anàlisi diferencial de l'empresa respecte a la ISO 27001 + ISO 27002

Al annex 1 trobem els 114 controls de la ISO/IEC 27002[1].

Tot seguit podem veure la presentació gràfica dels resultats de l'annex 1:



Imatge 3: Gràfic amb els valors CMM dels controls ISO 27002.



Imatge 4: Diagrama de radar amb els valors CMM dels controls ISO 27002.

Com podem veure als gràfics anteriors, les polítiques de seguretat de la companyia es troben en un estat inicial (<20%), els aspectes

organitzatius, seguretat lligada als RRHH, gestió d'actius, control d'accés, xifratge i la gestió d'incidents a la seguretat de la informació es troben en un estat més avançat però encara amb força treball per desenvolupar (>20%;<60%), per últim, tenim els aspectes més desenvolupats (>60%;<100%) on trobem la seguretat física i ambiental, seguretat en la operativa, seguretat en les telecomunicacions, adquisició, desenvolupament i manteniment dels sistemes de la informació, relacions amb subministradors, aspectes de la seguretat de la informació i el compliment.

Per tant, tenim que no s'està complint amb les polítiques de seguretat, els aspectes organitzatius, seguretat lligada als RRHH, gestió d'actius, control d'accés, xifratge i la gestió d'incidents a la seguretat de la informació.

1.5 Actius de la companyia

A la taula següent podem veure els diferents sistemes que tenim a la central de la companyia a la seu de Madrid:

Ubicació	Tipus	Serveis
Madrid – CPD Central	Software	Microsoft Exchange Server
		Microsoft Sharepoint Server
		ePO McAfee
		Aplicacions pròpies
		Microsoft Windows Server
		Microsoft ISA Server
		Symantec BackupExec
		Microsoft CRM
		Servidor de base de dades
		Gestió d'incidències
Núvol	Software	Microsoft Windows Server
		Microsoft Navision Dynamics
Madrid – Oficines	Software	Microsoft Windows
		Microsoft Office
		Software de càlcul i disseny
		Microsoft Navision Dynamics

Taula 1: Sistemes de la companyia.

Tot seguit tenim els actius que formen la part d'instal·lacions del CPD.

Ubicació	Tipus	Element
Madrid – CPD Central	Infraestructura	Racks de servidors
		Racks de comunicacions
		SAI
		Generador elèctric a gasoil
		Climatització
		Climatització de reserva
		Control d'accés
		Càmera de vigilància
		Sensors elèctrics i ambientals

Taula 2: Actius del CPD.

Per últim es realitza un inventari del hardware existent a la seu central.

Ubicació	Tipus	Element
Madrid – CPD Central	Hardware	Servidors de correu
		Servidors Web
		Servidor d'anti-virus
		Controlador de domini principal
		Controlador de domini secundari
		Firewall
		Servidor de còpies de seguretat
		Servidor CRM
		Servidors de dades
		NAS
		Cabina de cintes
		Servidors de desenvolupament
		Switches
		Routers
		Centraleta de telefonia IP
Núvol	Hardware	Servidor Navision Dynamics
		Controladors de domini secundaris
Madrid - Oficines	Hardware	Portàtils tècnics
		Portàtils no tècnics
		Equips sobretaula tècnics
		Equips sobretaula no tècnics
		Multifuncionals A3/A4 Color
		Plotters
		Switches
		Mòbils
		Telèfons fixes

Taula 3: Inventari de Hardware a la seu central.

2. Sistema de Gestió Documental:

2.1 Introducció

El Sistema de Gestió Documental del SGSI de l'empresa recull tota la documentació necessària per a la correcta implementació i manteniment del SGSI requerida per la norma ISO/IEC 27001:2013.

La norma ISO/IEC 27001 estableix la necessitat de generar i emmagatzemar en qualsevol suport els següents documents i registres[(2)]:

- Documents:
  - Abast del SGSI.
  - Polítiques i objectes de seguretat de la informació.
  - Metodologia d'avaluació i tractament de riscos.
  - Declaració d'aplicabilitat.
  - Pla de tractament del risc.
  - Informe d'avaluació de riscos.
  - Definició de funcions i responsabilitats de seguretat.
  - Inventari d'actius.
  - Ús acceptable dels actius.
  - Política de control d'accés.
  - Procediments operatius per a la gestió de TI.
  - Principis d'enginyeria per a sistema segur.
  - Política de seguretat per a proveïdors.
  - Procediment per a la gestió d'incidents.
  - Procediments de la continuïtat del negoci.
  - Requisits legals, normatius i contractuals.
- Registres:
  - Registres de capacitació, habilitats, experiència i qualificacions.
  - Resultats de supervisió i medició.
  - Programa d'auditoria interna.
  - Resultats de les auditories internes.
  - Resultats de la revisió per part de la direcció.

- Resultats d'accions correctives.
- Registres sobre activitats dels usuaris, excepcions i esdeveniments de seguretat.

Encara que al SGSI de la companyia ens centrarem en la documentació inclosa als apartats següents.

2.2 Política de Seguretat

A l'annex 2 podem veure la definició de la política de seguretat de la informació per a l'SGSI de la companyia i el llistat de les diferents polítiques.

2.3 Procediment d'Auditories Internes

La companyia ha de realitzar auditories internes[3] per verificar que els seus controls, processos, procediments i objectius compleixen amb els requeriments de la norma ISO/IEC 27001, aquestes auditories seran planificades periòdicament i no seran realitzades per personal involucrat en el propi treball a auditar.

Totes les auditories seran de fase 1 al tractar-se d'auditories internes, tot i que el personal auditor pot ser personal extern a la companyia.

A l'annex 3 podem veure en detall el procediment d'auditories internes.

2.4 Gestió d'Indicadors

A l'annex 4 podem veure el llistat d'indicadors per a avaluar els controls més crítics aplicats al SGSI de la companyia, per poder verificar l'eficiència del sistema.

2.5 Procediment de Revisió per Direcció

La direcció[4] de la companyia haurà de revisar el SGSI com a mínim un cop l'any, aquesta revisió servirà per comprovar la correcta instauració i eficàcia del sistema. La freqüència mínima de revisió per part de la direcció la marca la norma ISO/IEC 27001 al punt 7.

La imatge[5] següent ens mostra totes les entrades i sortides d'informació necessàries per a la revisió per la direcció:

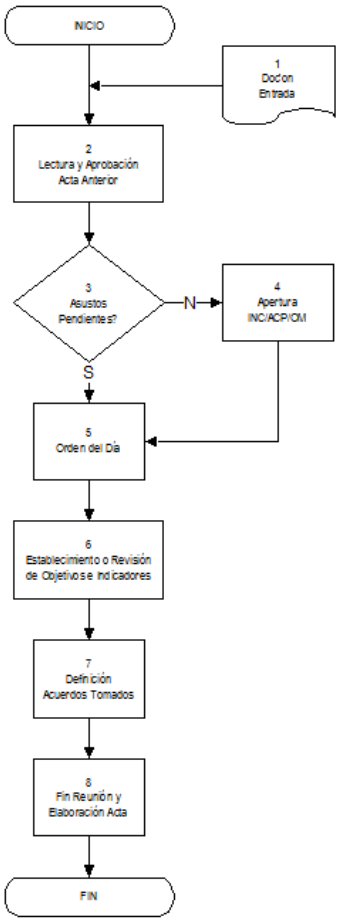
Imatge 5: Revisió del SGSI per la direcció. Font: Blog 5consultores.

Com mostra la imatge 5, les dades necessàries a revisar per la direcció inclouen:

- Resultats de revisions anteriors.
- Les enquestes als usuaris.
- Resultats dels indicadors.
- Accions correctives.
- Accions preventives.
- Accions de seguiment.

Un cop revisades les dades d'entrada, es generarà un informe amb els canvis que es poden dur a terme i les propostes de millora per augmentar l'eficàcia del SGSI.

La imatge[6] següent ens mostra el procediment a seguir per dur a terme la revisió del SGSI per part de la direcció:



Imatge 6: Procediment de revisió del SGSI per la direcció. Font: eGAM.

Tots els resultats de la revisió per la direcció es documentaran i s'inclouran al registre documental del SGSI.

2.6 Gestió de Rols i Responsabilitats

A l'annex 5 podem veure en detall els diferents rols i funcions del SGSI amb els seus responsables.

2.7 Metodologia d'Anàlisis de Riscos

Un anàlisi de riscos consisteix en una aproximació metòdica per poder determinar els riscos que té la companyia. Per realitzar una correcta metodologia d'Anàlisis de Riscos, farem servir MAGERIT v.3[7 - 8] amb les seves cinc fases ben diferenciades com es veu a la imatge[9] següent:

Imatge 7: Anàlisis de Riscos del SGSI. Font: José M. Poveda ISO 27001.

- **Fase 1: Actius:** dintre d'aquesta fase es realitzarà un inventari dels actius de la companyia. Considerarem actius a tots els elements que intervenen en el tractament de la informació. MAGERIT diferencia els actius en el següents tipus:
  - Actiu d'informació (Bases de dades, documentació...)
  - Software.
  - Hardware.
  - Xarxa.
  - Equipament auxiliar (SAI, aire acondicionat...).
  - Instal·lacions.
  - Serveis (connexió a Internet, accés telefònic...)
  - Personal.

  A l'annex 6 trobem les plantilles per a la realització del inventari d'actius Hardware i terminals mòbils de la companyia.

  Per a la valoració dels actius es fa servir una valoració qualitativa que podem veure a la taula següent:

Paràmetre d'avaluació d'actius	Valor		
Confidencialitat (C)	Baixa (1)	Mitjana (2)	Alta (3)
Integritat (I)	Baixa (1)	Mitjana (2)	Alta (3)
Disponibilitat (D)	Baixa (1)	Mitjana (2)	Alta (3)
Avaluació Final d'actius: (VA) = (C) * (I) * (D)	On 1 serà de poca importància i 27 serà de molta importància.		

Taula 4: Valoració qualitativa dels actius.

- **Fase 2: Amenaces:** es considera una amenaça a qualsevol situació que posi en risc la seguretat de la companyia. MAGERIT cataloga les amenaces dintre de les següents categories:
  - Desastres naturals [N]: foc, danys per aigua i desastres naturals.
  - D'origen industrial [I]: desastres industrials, avaria d'origen lògic o físic, tall en el subministrament elèctric...
  - Errors o fallides no intencionades [E]: errors dels usuaris, errors de l'administrador, errors de configuració...
  - Atacs deliberats [A]: manipulació de la configuració, abús dels privilegis d'accés, robatori d'equips...

  Les amenaces les podem classificar com es mostra a la taula següent:

Valor	Estimació de l'impacte de l'amenaça
1	Poc significativa: tindrà un baix impacte per a la companyia
2	Mitjana: tundra un impacte mitjà per a la companyia.
3	Alta significació: L'impacte per a la companyia serà alt.

Taula 5: Classificació de les amenaces.

Les amenaces aprofiten les vulnerabilitats del sistema per causar un impacte a la companyia. Es considera vulnerabilitat a un problema de seguretat que comporta un risc per a la companyia de sofrir una amenaça.

A la següent taula podem veure la probabilitat de que una amenaça s'aprofiti d'una vulnerabilitat per afectar a la seguretat del sistema:

Nivell	Valoració de la probabilitat de que una amenaça pugui aprofitar una vulnerabilitat.
1	La probabilitat de dany és molt baix. És possible que l'amenaça no pugui aprofitar cap vulnerabilitat.
2	La probabilitat de dany és baix. És possible que l'amenaça no pugui aprofitar cap vulnerabilitat.

Nivell	Valoració de la probabilitat de que una amenaça pugui aprofitar una vulnerabilitat.
3	La probabilitat de dany és mitjana. És possible que l'amenaça pugui aprofitar una vulnerabilitat un cop l'any.
4	La probabilitat de dany és alta. És possible que l'amenaça pugui aprofitar una vulnerabilitat més d'un cop l'any.
5	La probabilitat de dany és molt alta. És possible que l'amenaça pugui aprofitar una vulnerabilitat molts cops l'any.

Taula 6: Valoració d'amenaça que aprofita una vulnerabilitat del sistema.

Un cop tenim feta la valoració de les amenaces i de les vulnerabilitats de la companyia, podem realitzar una valoració de l'impacte que tindria la companyia si es produís alguna de les amenaces avaluades. L'impacte és el percentatge del actiu que es perdrà en cas d'amenaça. La valoració de l'impacte es realitza únicament sobre els actius essencials de la companyia. A la taula següent podem veure els diferents nivells d'impacte:

Nivell d'impacte	Valor afectat
1	Molt baix (0%-10%)
2	Baix (10%-25%)
3	Mitjà (25%-45%)
4	Alt (45%-75%)
5	Molt alt (75%-100%)

Taula 7: Nivells d'impacte en cas d'amenaça.

- **Fase 3: Salvaguardes:** segons MAGERIT, una salvaguarda és qualsevol procediment per minimitzar el risc d'impacte per amenaces. Les salvaguardes es podem classificar segons el seu efecte:
  - Reduint la probabilitat d'amenaça.
  - Reduint l'impacte causat.
- **Fase 4: Impacte residual:** un cop definides les amenaces i tenint en compte les salvaguardes del sistema, tornem a calcular l'impacte sobre tots els actius. Aquest nou impacte hauria de ser molt inferior al anterior degut a que amb les salvaguardes em disminuït la probabilitat de que es produeixi una amenaça, reduint l'impacte en cas de que aquest es doni.
- **Fase 5: Risc residual:** un cop calculat l'impacte residual, obtenim el risc residual. Aquest risc ha de poder ser assumit per la

companyia i es troba per sota d'un llindar en que el cost és superior al benefici per poder millorar la seguretat.

2.8 Declaració d'Aplicabilitat

A l'annex 7 podem veure la declaració d'aplicabilitat per als 114 controls de la norma ISO/IEC 27002:2013 sobre el sistema SGSI de la companyia i la documentació relacionada amb els mateixos.

3. Anàlisis de Riscos

3.1 Introducció

A aquesta fase del SGSI s'ha de realitzar un anàlisis de riscos per tal d'identificar els riscos als que s'exposa la companyia, per seleccionar les mesures de seguretat a aplicar en funció d'aquests riscos i així poder elaborar un pla de contingència.
Aquests anàlisi de riscos ens serà necessari per poder obtindre la certificació de la ISO/IEC 27001.

3.2 Inventari d'actius, valoració i dimensió de seguretat

La primera fase per poder realitzar un anàlisi de riscos, consisteix en la realització de l'inventari dels actius per tal de conèixer tots els elements que necessita la companyia per poder desenvolupar les seves tasques. També hem de conèixer quin és el valor de l'actiu per a la companyia, per a que el cost de la seguretat per protegir-lo no superi al cost del propi actiu.

Aquest inventari es realitzarà fent servir la metodologia MAGERIT elaborada pel Ministeri d'Administracions Públiques. Així mateix, farem servir la següent taula per a la valoració de l'impacte sobre els actius:

		Degradació de l'actiu		
		1%	**10%**	**100%**
Valor de l'actiu	**Molt Alt**	Mig	Alt	Molt Alt
	Alt	Baix	Mig	Alt
	Mig	Molt Baix	Baix	Mig
	Baix	Molt Baix	Molt Baix	Baix
	Molt Baix	Molt Baix	Molt Baix	Molt Baix

Taula 8: Valoració de l'impacte sobre els actius.

Per altra banda es farà servir la següent taula per definir els valors ACIDA (Autenticitat, Confidencialitat, Integritat, Disponibilitat, Auditabilitat) de les cinc dimensions de seguretat:

Dimensió de seguretat		
Valor de l'actiu	**Valor**	**Criteri**
Molt Alt	10	Dany molt greu a la companyia
Alt	7-9	Dany greu a la companyia
Mig	4-6	Dany important a la companyia
Baix	1-3	Dany menor a la companyia
Molt Baix	0	Dany irrellevant a la companyia

Taula 9: Dimensió de seguretat.

A la taula resum següent podem veure l'inventari, la valoració i la dimensió de seguretat dels actius de la companyia agrupats pels diferents àmbits:

Àmbit	Actiu	Valor d'actiu	Aspectes crítics				
			A	C	I	D	A
Instal·lacions							
	Oficines centrals de la companyia	10	9	9	9	9	8
Hardware							
	Servidor de correu	8	8	8	8	8	8
	Servidor Web	5	6	6	6	5	5
	Servidor d'antivirus	3	6	4	4	3	4
	Controlador de domini principal	6	7	7	6	4	6
	Controlador de domini secundari	4	7	7	5	3	5
	Firewall	6	6	6	5	5	6
	Servidor de còpies de seguretat	3	5	5	4	4	4
	Servidor CRM	9	8	8	8	8	8
	Servidor de base de dades	6	7	7	7	7	6
	Servidor de dades	9	8	8	8	8	4
	NAS	9	8	8	8	8	2
	Servidors de desenvolupament	0	4	1	1	1	1
	Switches CPD	8	8	8	8	8	2
	Switches	2	4	2	4	4	1
	Routers	6	6	2	5	6	3
	Servidor Navision Dynamics	9	8	8	8	8	8
	Controlador de domini secundari al núvol	2	7	7	5	2	5
	Portàtils tècnics	2	6	5	2	2	1
	Portàtils no tècnics	1	6	5	2	2	1
	Equips sobretaula tècnics	2	6	5	2	2	1
	Equips sobretaula no tècnics	1	6	5	2	2	1
	Multifuncionals A3/A4 color	0	4	2	2	4	1
	Plotters	1	4	2	4	4	1
	Mòbils	0	4	4	2	3	1
	Telèfons fixes	0	3	2	2	2	0
	Centraleta de telefonia IP	5	6	6	5	6	2
Aplicació							
	Microsoft Exchange Server	8	8	8	8	8	8
	Microsoft SharePoint Server	3	7	7	6	4	6
	ePO McAfee	3	5	4	5	3	4
	Aplicació pròpia d'inventari	0	6	4	2	2	1
	Aplicació pròpia d'alta i baixa d'usuaris	0	6	6	2	2	1
	Aplicació pròpia d'inventari de mòbils	0	6	4	2	2	1
	Microsoft Windows Server	6	8	4	6	7	2
	Microsoft ISA Server	6	8	4	5	8	6
	Symantec BackupExec	3	8	2	2	2	3

Àmbit	Actiu	Valor d'actiu	Aspectes crítics				
			A	C	I	D	A
	Microsoft CRM	9	8	8	8	8	8
	Microsoft Navision Dynamics	9	8	8	8	8	8
	Microsoft Windows	2	6	2	5	5	2
	Microsoft Office	0	6	1	3	3	1
	Gestió d'incidències	0	6	1	2	2	3
	Aplicacions de càlcul	5	7	6	6	4	1
	Aplicacions de disseny	5	7	6	6	4	1
Dades							
	Projectes propis	10	10	10	10	10	10
	Base de dades CRM	10	10	10	10	10	10
	Base de dades de personal	6	7	9	8	6	4
	Base de dades Navision Dynamics	8	8	8	8	8	7
	Codi font aplicació pròpia d'inventari	4	7	8	8	5	2
	Codi font aplicació pròpia d'alta i baixa d'usuaris	4	7	8	8	5	2
	Codi font aplicació pròpia d'inventari de mòbils	4	7	8	8	5	2
Xarxa							
	Línies RTB	3	8	1	1	5	0
	Línies RDSI	7	8	7	8	8	1
	Internet fibra òptica	8	8	8	8	8	6
	LAN	8	8	8	8	8	8
	VPN	7	8	8	7	6	7
Serveis							
	Correu electrònic	8	9	9	9	9	7
	Intranet	3	8	6	5	3	3
	Emmagatzematge de dades	9	9	9	9	9	8
	Teletreball	3	8	8	6	3	3
Equipament auxiliar							
	Racks de servidors	0	3	1	1	1	0
	Racks de comunicacions	0	3	1	1	1	0
	SAI	6	6	3	8	8	1
	Generador elèctric a gasoil	4	6	3	7	7	1
	Climatització	6	8	3	8	9	1
	Climatització de reserva	4	8	3	7	7	1
	Control d'accés	6	8	6	7	3	1
	Càmeres de vigilància	3	6	5	4	3	1
	Sensors elèctrics i ambientals	2	5	1	4	4	1
Personal							
	Usuaris interns	10	10	9	10	10	9
	Administradors de sistemes	10	10	10	10	10	10
	Programadors	8	10	10	9	6	8
	Proveidors	7	10	10	10	7	8

Taula 10: Inventari, valoració i dimensió de seguretat ACIDA dels actius.

3.3 Anàlisi d'amenaces

Segons la norma UNE 71504:2008, una amenaça és la causa potencial d'un incident que pot causar danys a un sistema d'informació o a una organització.

Farem servir MAGERIT per a la realització de l'anàlisi d'amenaces, on trobem la següent classificació:

- Desastres naturals.
- D'origen industrial.
- Errors i fallides no intencionats.
- Atacs intencionats.

Farem servir la següent taula per a assignar els valors de la freqüència amb la que ocorre una amenaça:

Freqüència Amenaça		
Freqüència	**Valor**	**Criteri**
Molt Alt	10	Diariament
Alt	7-9	Mensualment
Mig	4-6	Un cop l'any
Baix	1-3	Menor d'un cop l'any
Molt Baix	0,1	Gairebé mai

Taula 11: Freqüència de les amenaces.

A la taula següent podem veure per a cada actiu el tipus d'amenaça catalogada en MAGERIT que pot afectar a la companyia (fent servir la codificació MAGERIT, veure annex 8), la freqüència en la que pot ocorre, i l'impacte a les diferents dimensions de la seguretat amb els valors ACIDA:

Àmbit	Actiu	ID MAGERIT amenaça	Freqüència amenaça	Impacte				
				A	C	I	D	A
Instal·lacions								
	Oficines centrals de la companyia	N.1	0.1				100%	
		N.2	1				100%	
		N.*	0.1				100%	
		I.1	0.1				100%	
		I.2	0.1				80%	
		I.*	0.1				50%	
		A.11	0.1		5%	15%		
Hardware								
	- Servidor de correu - Servidor CRM - Servidor de dades - NAS - Switches CPD - Servidor Navision Dynamics	N.1	0.1				100%	
		N.2	1				100%	
		N.*	0.1				100%	
		I.1	0.1				100%	
		I.2	0.1				80%	
		I.*	0.1				50%	
		I.5	3				30%	
		I.6	3				25%	
		I.7	1				15%	
		E.2	1		40%	50%	5%	
		E.23	1				10%	
		E.24	1				5%	
		A.6	1		75%	75%	50%	
		A.7	0.1		10%	15%	5%	
		A.11	0.1		75%	80%		
		A.23	0.1		75%		75%	
		A.24	1				10%	
		A.25	0.1		50%		100%	
		A.26	0.1				90%	
	- Servidor de Web - Controlador de	N.1	0.1				100%	
		N.2	1				100%	

Àmbit	Actiu	ID MAGERIT amenaça	Freqüència amenaça	Impacte				
				A	C	I	D	A
	domini principal - Firewall - Servidor de base de dades - Routers - Centraleta de telefonia IP	N.*	0.1				100%	
		I.1	0.1				100%	
		I.2	0.1				80%	
		I.*	0.1				50%	
		I.5	3				20%	
		I.6	3				10%	
		I.7	1				5%	
		E.2	1		20%	25%	5%	
		E.23	1				5%	
		E.24	1				5%	
		A.6	1		75%	50%	40%	
		A.7	0.1		5%	10%	5%	
		A.11	0.1		50%	75%		
		A.23	0.1		50%		50%	
		A.24	1				5%	
		A.25	0.1		65%		65%	
		A.26	0.1				75%	
	- Servidor d'antivirus - Controlador de domini secundari - Servidor de còpies de seguretat - Switches - Controlador de domini secundari al núvol - Portàtils tècnics - Portàtils no tècnics - Equips sobretaula tècnics - Equips sobretaula no tècnics	N.1	0.1				100%	
		N.2	1				100%	
		N.*	0.1				100%	
		I.1	0.1				100%	
		I.2	0.1				80%	
		I.*	0.1				50%	
		I.5	5				5%	
		I.6	3				5%	
		I.7	1				5%	
		E.2	1		5%	5%	5%	
		E.23	1				5%	
		E.24	3				5%	
		A.6	1		25%	25%	5%	
		A.7	3		5%	5%	5%	
		A.11	0.1		25%	25%		
		A.23	0.1		25%		10%	
		A.24	2				5%	
		A.25	2		50%		50%	
		A.26	0.1				50%	
	- Servidors de desenvolupament - Multifuncionals A3/A4 color - Plotters - Mòbils - Telèfons fixes	N.1	0.1				100%	
		N.2	1				100%	
		N.*	0.1				100%	
		I.1	0.1				100%	
		I.2	0.1				80%	
		I.*	0.1				50%	
		I.5	4				10%	
		I.6	3				5%	
		I.7	1				5%	
		E.2	1		5%	5%	5%	
		E.23	3				10%	
		E.24	4				5%	
		A.6	1		5%	5%	5%	
		A.7	4		5%	5%	5%	
		A.11	0.1		5%	5%		
		A.23	0.1		10%		5%	
		A.24	2				5%	
		A.25	2		25%		5%	
		A.26	0.1				10%	
Aplicació								
	- Microsoft Exchange Server - Microsoft CRM - Microsoft Navision Dynamics	I.5	0.1				50%	
		E.1	4		25%	25%	50%	
		E.2	1		10%	10%	25%	
		E.8	0.1		50%	45%	50%	
		E.15	0.1			50%		

Àmbit	Actiu	ID MAGERIT amenaça	Freqüència amenaça	Impacte				
				A	C	I	D	A
	- Microsoft Windows Server	E.18	0.1				80%	
		E.19	0.1		60%			
		E.20	0.1		40%	35%	40%	
		E.21	1			25%	25%	
		A.5	0.1	25%	25%	35%		
		A.6	0.1		40%	35%	40%	
		A.7	1		25%	20%	10%	
		A.8	0.1		45%	50%	40%	
		A.9	0.1		50%			
		A.10	0.1			50%		
		A.15	0.1			75%		
		A.18	0.1				100%	
		A.19	0.1		75%			
		A.22	0.1		50%	60%	50%	
	- ePO McAfee - Microsoft ISA Server - Microsoft Windows - Aplicacions de càlcul - Aplicacions de disseny	I.5	0.1				35%	
		E.1	4		15%	15%	25%	
		E.2	1		5%	5%	10%	
		E.8	0.1		30%	25%	25%	
		E.15	0.1			25%		
		E.18	0.1				25%	
		E.19	0.1		25%			
		E.20	0.1		25%	15%	25%	
		E.21	1			10%	10%	
		A.5	0.1	25%	25%	35%		
		A.6	0.1		30%	25%	20%	
		A.7	1		10%	10%	10%	
		A.8	0.1		30%	30%	25%	
		A.9	0.1		50%			
		A.10	0.1			35%		
		A.15	0.1			50%		
		A.18	0.1				50%	
		A.19	0.1		50%			
		A.22	0.1		50%	35%	35%	
	- Microsoft SharePoint Server - Symantec BackupExec - Aplicació pròpia d'inventari - Aplicació pròpia d'alta i baixa d'usuaris - Aplicació pròpia d'inventari de mòbils - Microsoft Office - Gestió d'incidències	I.5	0.1				35%	
		E.1	0.1		0%	0%	0%	
		E.2	1		10%	5%	5%	
		E.8	0.1		25%	20%	20%-	
		E.15	0.1			25%		
		E.18	0.1				25%	
		E.19	0.1		35%			
		E.20	0.1		10%	15%	5%	
		E.21	1			5%	5%	
		A.5	0.1	45%	45%	25%		
		A.6	0.1		45%	45%	35%	
		A.7	1		5%	5%	5%	
		A.8	0.1		10%	10%	10%	
		A.9	0.1		5%			
		A.10	0.1			5%		
		A.15	0.1			35%		
		A.18	0.1				40%	
		A.19	0.1		30%			
		A.22	0.1		25%	25%	25%	
Dades								
	- Projectes propis - Base de dades CRM - Base de dades Navision Dynamics - Base de dades de personal	E.1	5		75%	75%	75%	
		E.2	1		50%	50%	80%	
		E.15	5			45%		
		E.18	0.1				90%	
		E.19	0.1		80%			
		A.5	0.1	65%	50%	50%		
		A.6	0.1		75%	75%	50%	
		A.11	0.1		80%	75%		

Àmbit	Actiu	ID MAGERIT amenaça	Freqüència amenaça	Impacte				
				A	C	I	D	A
		A.15	0.1			90%		
		A.18	0.1			90%		
		A.19	0.1				50%	
	- Codi font aplicació pròpia d'inventari - Codi font aplicació pròpia d'alta i baixa d'usuaris - Codi font d'aplicació pròpia d'inventari de mòbils	E.1	0.1		50%	50%	50%	
		E.2	1		30%	30%	50%	
		E.15	0.1			25%		
		E.18	0.1				50%	
		E.19	0.1		10%			
		A.5	0.1	5%	5%	5%		
		A.6	0.1		10%	10%	5%	
		A.11	0.1		5%	5%		
		A.15	0.1			50%		
		A.18	0.1			50%		
		A.19	0.1				15%	
Xarxa								
	Línies RTB	I.8	0.1				75%	
		A.7	1		5%	5%	5%	
		A.14	0.1		2%			
		A.19	0.1				0%	
	Línies RDSI	I.8	0.1				85%	
		A.7	10		5%	5%	5%	
		A.14	0.1		2%			
		A.19	0.1				0%	
	- Internet fibra òptica - LAN - VPN	I.8	0.1				90%	
		E.2	0.1		25%	10%	5%	
		E.9	0.1		50%			
		E.10	0.1			45%		
		E.15	0.1			5%		
		E.18	0.1				5%	
		E.19	0.1		20%			
		E.24	1				5%	
		A.5	0.1	50%	50%	25%		
		A.6	0.1		25%	25%	20%	
		A.7	10		5%	5%	5%	
		A.9	0.1		50%			
		A.10	0.1			35%		
		A.11	0.1		80%	60%		
		A.12	0.1		75%			
		A.14	0.1		75%			
		A.15	0.1			45%		
		A.19	0.1		45%			
		A.24	1				5%	
Serveis								
	- Correu electrònic - Emmagatzematge de dades - Intranet - Teletreball	E.1	4		25%	25%	10%	
		E.2	1		10%	15%	10%	
		E.9	0.1		45%			
		E.10	0.1			35%		
		E.15	1			45%		
		E.18	0.1				80%	
		E.19	0.1		50%			
		E.24	1				25%	
		A.5	0.1	50%	50%	50%		
		A.6	0.1		50%	50%	10%	
		A.7	7		25%	25%	5%	
		A.9	1		50%			
		A.10	0.1			35%		
		A.11	0.1		75%	75%		
		A.13	1			25%		
		A.15	0.1			75%		
		A.18	0.1				90%	
		A.19	0.1		50%			

Àmbit	Actiu	ID MAGERIT amenaça	Freqüència amenaça	Impacte				
				A	C	I	D	A
		A.24	1				25%	
Equipament auxiliar								
	- Racks de servidors - Racks de comunicacions	N.1	0.1				100%	
		N.2	1				100%	
		N.*	0.1				100%	
		I.1	0.1				100%	
		I.2	0.1				80%	
		I.*	0.1				50%	
		A.11	0.1		10%	10%		
		A.23	0.1		5%		5%	
		A.25	0.1		5%		5%	
		A.26	0.1				5%	
	- SAI - Generador elèctric a gasoil - Climatització - Climatització de reserva - Control d'accés - Càmeres de vigilància - Sensors elèctrics i ambientals	N.1	0.1				100%	
		N.2	1				100%	
		N.*	0.1				100%	
		I.1	0.1				100%	
		I.2	0.1				80%	
		I.*	0.1				50%	
		I.5	1				15%	
		I.6	1				15%	
		I.9	1				15%	
		E.23	1				10%	
		A.11	0.1		15%	25%		
		A.23	0.1		15%		15%	
		A.25	0.1		25%		15%	
		A.26	0.1				15%	
Personal								
	- Usuaris interns - Administradors de sistemes - Programadors	E.7	5				10%	
		E.19	0.1		75%			
		E.28	3				5%	
		A.28	0.1				10%	
		A.29	0.1		50%	50%	5%	
		A.30	0.1		50%	50%	5%	
	- Proveïdors	E.7	4				10%	
		E.19	0.1		5%			
		E.28	3				2%	
		A.28	0.1				5%	
		A.29	0.1		15%	15%	2%	
		A.30	0.1		15%	15%	2%	

Taula 12: Amenaces, freqüència i impacte ACIDT per als actius.

3.4 Impacte potencial

Parlem d'impacte potencial com l'efecte que tindria una amenaça en materialitzar-se sobre un actiu de la companyia abans d'aplicar les contramesures.

A la taula següent (calculada amb l'Excel "Calcul_ImpactePotencial_Risc_Projectes.xlsx" full Impacte_Potencial), determinarem l'impacte potencial fent servir els resultats de la taula 10 i la taula 12 amb els valors més alts de l'impacte per a cada actiu de la companyia. Utilitzarem la fórmula:

Impacte potencial = Valor_Actiu * Impacte

Àmbit	Actiu	Aspectes crítics					Impacte màxim amenaça					Impacte potencial				
		A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
Instal·lacions																
	Oficines centrals de la companyia	9	9	9	9	8		5%	15%	100%			0.45	1.35	9	
Hardware																
	Servidor de correu	8	8	8	8	8		75%	75%	100%			6	6	8	
	Servidor Web	6	6	6	5	5		75%	75%	100%			4.5	4.5	5	
	Servidor d'antivirus	6	4	4	3	4		50%	25%	100%			2	1	3	
	Controlador de domini principal	7	7	6	4	6		75%	75%	100%			5.25	4.5	4	
	Controlador de domini secundari	7	7	5	3	5		50%	25%	100%			3.5	1.25	3	
	Firewall	6	6	5	5	6		75%	75%	100%			4.5	3.75	5	
	Servidor de còpies de seguretat	5	5	4	4	4		50%	25%	100%			2.5	1	4	
	Servidor CRM	8	8	8	8	8		75%	75%	100%			6	6	8	
	Servidor de base de dades	7	7	7	7	6		75%	75%	100%			5.25	5.25	7	
	Servidor de dades	8	8	8	8	4		75%	75%	100%			6	6	8	
	NAS	8	8	8	8	2		75%	75%	100%			6	6	8	
	Servidors de desenvolupament	4	1	1	1	1		25%	5%	100%			0.25	0.05	1	
	Switches CPD	8	8	8	8	2		75%	75%	100%			6	6	8	
	Switches	4	2	4	4	1		50%	25%	100%			1	1	4	
	Routers	6	2	5	6	3		75%	75%	100%			1.5	3.75	6	
	Servidor Navision Dynamics	8	8	8	8	8		75%	75%	100%			6	6	8	
	Controlador de domini secundari al núvol	7	7	5	2	5		50%	25%	100%			3.5	1.25	2	
	Portàtils tècnics	6	5	2	2	1		50%	25%	100%			2.5	0.5	2	
	Portàtils no tècnics	6	5	2	2	1		50%	25%	100%			2.5	0.5	2	
	Equips sobretaula tècnics	6	5	2	2	1		50%	25%	100%			2.5	0.5	2	
	Equips sobretaula no tècnics	6	5	2	2	1		50%	25%	100%			2.5	0.5	2	
	Multifuncionals A3/A4 color	4	2	2	4	1		25%	5%	100%			0.5	0.1	4	
	Plotters	4	2	4	4	1		25%	5%	100%			0.5	0.2	4	

Àmbit	Actiu	Aspectes crítics					Impacte màxim amenaça					Impacte potencial				
		A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
	Mòbils	4	4	2	3	1		25%	5%	100%			1	0.1	3	
	Telèfons fixes	3	2	2	2	0		25%	5%	100%			0.5	0.1	2	
	Centraleta de telefonia IP	6	6	5	6	2		75%	75%	100%			4.5	3.75	6	
Aplicació																
	Microsoft Exchange Server	8	8	8	8	8	25%	75%	75%	100%		2	6	6	8	
	Microsoft SharePoint Server	7	7	6	4	6	45%	45%	45%	40%		3.15	3.15	2.7	1.6	
	ePO McAfee	5	4	5	3	4	25%	50%	50%	50%		1.25	2	2.5	1.5	
	Aplicació pròpia d'inventari	6	4	2	2	1	45%	45%	45%	40%		2.7	1.8	0.9	0.8	
	Aplicació pròpia d'alta i baixa d'usuaris	6	6	2	2	1	45%	45%	45%	40%		2.7	2.7	0.9	0.8	
	Aplicació pròpia d'inventari de mòbils	6	4	2	2	1	45%	45%	45%	40%		2.7	1.8	0.9	0.8	
	Microsoft Windows Server	8	4	6	7	2	25%	75%	75%	100%		2	3	4.5	7	
	Microsoft ISA Server	8	4	5	8	6	25%	50%	50%	50%		2	2	2.5	4	
	Symantec BackupExec	8	2	2	2	3	45%	45%	45%	40%		3.6	0.9	0.9	0.8	
	Microsoft CRM	8	8	8	8	8	25%	75%	75%	100%		2	6	6	8	
	Microsoft Navision Dynamics	8	8	8	8	8	25%	75%	75%	100%		2	6	6	8	
	Microsoft Windows	6	2	5	5	2	25%	50%	50%	50%		1.5	1	2.5	2.5	
	Microsoft Office	6	1	3	3	1	45%	45%	45%	40%		2.7	0.45	1.35	1.20	
	Gestió d'incidències	6	1	2	2	3	45%	45%	45%	40%		2.7	0.45	0.9	0.8	
	Aplicacions de càlcul	7	6	6	4	1	25%	50%	50%	50%		1.75	3	3	2	
	Aplicacions de disseny	7	6	6	4	1	25%	50%	50%	50%		1.75	3	3	2	
Dades																
	Projectes propis	10	10	10	10	10	65%	80%	90%	90%		6.5	8	9	9	
	Base de dades CRM	10	10	10	10	10	65%	80%	90%	90%		6.5	8	9	9	
	Base de dades de personal	7	9	8	6	4	65%	80%	90%	90%		4.55	7.2	7.2	5.4	
	Base de dades Navision Dynamics	8	8	8	8	7	65%	80%	90%	90%		5.2	6.4	7.2	6.3	
	Codi font aplicació pròpia d'inventari	7	8	8	5	2	5%	50%	50%	50%		0.35	4	4	2.5	

Àmbit	Actiu	Aspectes crítics					Impacte màxim amenaça					Impacte potencial				
		A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
	Codi font aplicació pròpia d'alta i baixa d'usuaris	7	8	8	5	2	5%	50%	50%	50%		0.35	4	4	2.5	
	Codi font aplicació pròpia d'inventari de mòbils	7	8	8	5	2	5%	50%	50%	50%		0.35	4	4	2.5	
Xarxa																
	Línies RTB	8	1	1	5	0		5%	5%	75%			0.05	0.05	3.75	
	Línies RDSI	8	7	8	8	1		5%	5%	85%			0.35	0.40	6.8	
	Internet fibra òptica	8	8	8	8	6	50%	80%	60%	90%		4	6.4	4.80	7.2	
	LAN	8	8	8	8	8	50%	80%	60%	90%		4	6.4	4.8	7.2	
	VPN	8	8	7	6	7	50%	80%	60%	90%		4	6.4	4.2	5.4	
Serveis																
	Correu electrònic	9	9	9	9	7	50%	75%	75%	90%		4.5	6.75	6.75	8.1	
	Intranet	8	6	5	3	3	50%	75%	75%	90%		4	4.5	3.75	2.7	
	Emmagatzematge de dades	9	9	9	9	8	50%	75%	75%	90%		4.5	6.75	6.75	8.1	
	Teletreball	8	8	6	3	3	50%	75%	75%	90%		4	6	4.5	2.7	
Equipament auxiliar																
	Racks de servidors	3	1	1	1	0		10%	10%	100%			0.1	0.1	1	
	Racks de comunicacions	3	1	1	1	0		10%	10%	100%			0.1	0.1	1	
	SAI	6	3	8	8	1		25%	25%	100%			0.75	2	8	
	Generador elèctric a gasoil	6	3	7	7	1		25%	25%	100%			0.75	1.75	7	
	Climatització	8	3	8	9	1		25%	25%	100%			0.75	2	9	
	Climatització de reserva	8	3	7	7	1		25%	25%	100%			0.75	1.75	7	
	Control d'accés	8	6	7	3	1		25%	25%	100%			1.5	1.75	3	
	Càmeres de vigilància	6	5	4	3	1		25%	25%	100%			1.25	1	3	
	Sensors elèctrics i ambientals	5	1	4	4	1		25%	25%	100%			0.25	1	4	
Personal																
	Usuaris interns	10	9	10	10	9		75%	50%	10%			6.75	5	1	
	Administradors de sistemes	10	10	10	10	10		75%	50%	10%			7.5	5	1	
	Programadors	10	10	9	6	8		75%	50%	10%			7.5	4.5	0.6	
	Proveïdors	10	10	10	7	8		15%	15%	10%			1.5	1.5	0.7	

Taula 13: Impacte potencial.

3.5 Nivell de risc Acceptable i risc Residual

El risc Acceptable d'una companyia és el que es pot assumir sense arribar a prendre mesures per reduir-lo. Per altra banda tenim que el risc Residual serà el que quedarà un cop aplicades les mesures i passats els controls.

El risc Acceptable de la companyia ha de ser aprovat per la Direcció i s'han d'indicar els criteris que s'han seguit per a definir aquest risc.

La Direcció de la companyia acceptarà un nivell de risc amb les característiques següents:

- Valor de l'actiu 5 que equival a un actiu de valor mig (4 – 6), la seva pèrdua causaria un dany important a la companyia.
- Impacte del 40%, ja que l'impacte pot anar des d'un 0% fins a un 100%.
- Freqüència 8 que equival a una freqüència mensual.

Per tant, tenim que es pot arribar fins a un nivell de risc de com a màxim 16 per a no aplicar mesures.

La fórmula que s'ha seguit per al càlcul del risc és la següent:

Risc = Impacte Potencial * Freqüència

A la taula següent (calculada amb l'Excel "Calcul_ImpactePotencial_Risc_Projectes.xlsx" full Calcul_Risc), podem veure els diferents nivells de risc per a cada actiu. S'han fet servir els resultats de la taula 12 utilitzant els valors de freqüència més alts i la taula 13 amb els valors de l'impacte potencial:

Àmbit	Actiu	Freqüència	Impacte potencial					Risc				
			A	C	I	D	A	A	C	I	D	A
Instal·lacions												
	Oficines centrals de la companyia	1		0.45	1.35	9			0.45	1.35	9	
Hardware												
	Servidor de correu	3		6	6	8			18	18	24	
	Servidor Web	3		4.5	4.5	5			13.5	13.5	15	
	Servidor d'antivirus	3		2	1	3			6	3	9	
	Controlador de domini principal	5		5.25	4.5	4			26.25	22.5	20	
	Controlador de domini secundari	5		3.5	1.25	3			17.5	6.25	15	
	Firewall	3		4.5	3.75	5			13.5	22.5	15	
	Servidor de còpies de seguretat	5		2.5	1	4			12.5	5	20	

Àmbit	Actiu	Freqüència	Impacte potencial					Risc				
			A	C	I	D	A	A	C	I	D	A
	Servidor CRM	3		6	6	8			18	18	24	
	Servidor de base de dades	3		5.25	5.25	7			15.75	15.75	21	
	Servidor de dades	3		6	6	8			18	18	24	
	NAS	3		6	6	8			18	18	24	
	Servidors de desenvolupament	4		0.25	0.05	1			1	0.20	4	
	Switches CPD	3		6	6	8			18	18	24	
	Switches	5		1	1	4			5	5	20	
	Routers	3		1.5	3.75	6			4.5	11.25	18	
	Servidor Navision Dynamics	3		6	6	8			18	18	24	
	Controlador de domini secundari al núvol	5		3.5	1.25	2			17.5	6.25	10	
	Portàtils tècnics	5		2.5	0.5	2			12.5	2.5	10	
	Portàtils no tècnics	5		2.5	0.5	2			12.5	2.5	10	
	Equips sobretaula tècnics	5		2.5	0.5	2			12.5	2.5	10	
	Equips sobretaula no tècnics	5		2.5	0.5	2			12.5	2.5	10	
	Multifuncionals A3/A4 color	4		0.5	0.1	4			2	0.4	16	
	Plotters	4		0.5	0.2	4			2	0.8	16	
	Mòbils	4		1	0.1	3			4	0.4	12	
	Telèfons fixes	4		0.5	0.1	2			2	0.4	8	
	Centraleta de telefonia IP	3		4.5	3.75	6			13.5	11.25	18	
Aplicació												
	Microsoft Exchange Server	4	2	6	6	8		8	24	24	32	
	Microsoft SharePoint Server	1	3.15	3.15	2.7	1.6		3.15	3.15	2.7	1.6	
	ePO McAfee	4	1.25	2	2.5	1.5		5	8	10	6	
	Aplicació pròpia d'inventari	1	2.7	1.8	0.9	0.8		2.7	1.8	0.9	0.8	
	Aplicació pròpia d'alta i baixa d'usuaris	1	2.7	2.7	0.9	0.8		2.7	2.7	0.9	0.8	
	Aplicació pròpia d'inventari de mòbils	1	2.7	1.8	0.9	0.8		2.7	1.8	0.9	0.8	
	Microsoft Windows Server	4	2	3	4.5	7		8	12	18	28	
	Microsoft ISA Server	4	2	2	2.5	4		8	4	10	16	
	Symantec BackupExec	1	3.6	0.9	0.9	0.8		3.6	0.9	0.9	0.8	
	Microsoft CRM	4	2	6	6	8		8	24	24	32	
	Microsoft Navision Dynamics	4	2	6	6	8		8	24	24	32	
	Microsoft Windows	4	1.5	1	2.5	2.5		6	4	10	10	
	Microsoft Office	1	2.7	0.45	1.35	1.20		2.7	0.45	1.35	1.20	
	Gestió d'incidències	1	2.7	0.45	0.9	0.8		2.7	0.45	0.9	0.8	
	Aplicacions de càlcul	4	1.75	3	3	2		7	12	12	8	
	Aplicacions de disseny	4	1.75	3	3	2		7	12	12	8	

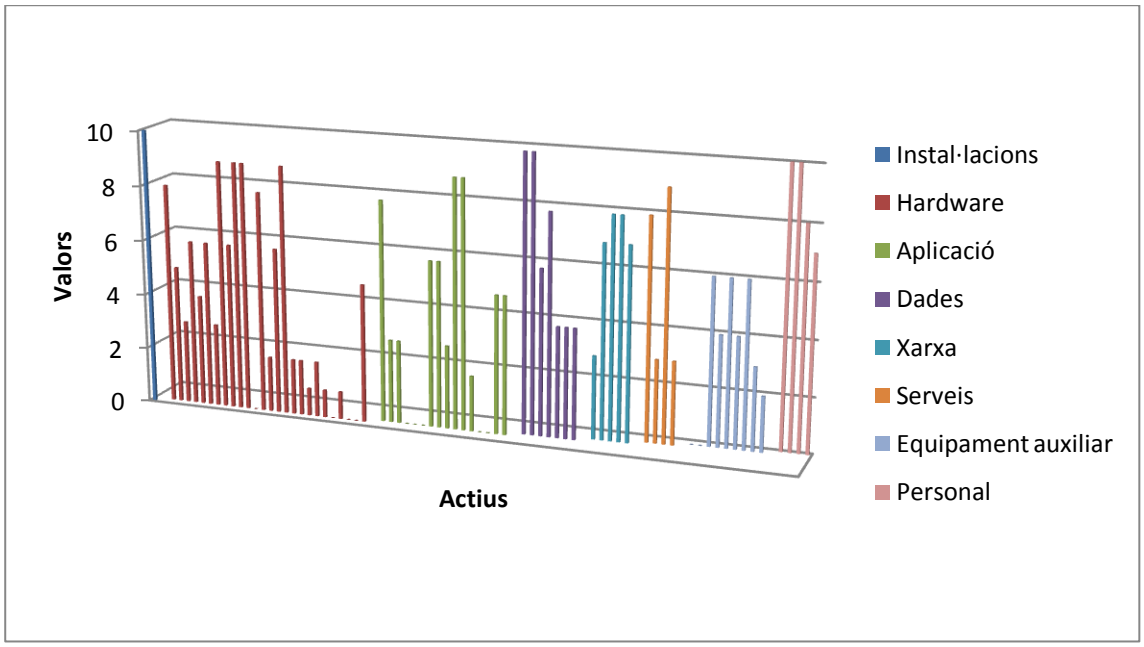
Àmbit	Actiu	Freqüència	Impacte potencial					Risc				
			A	C	I	D	A	A	C	I	D	A
Dades												
	Projectes propis	5	6.5	8	9	9		32.5	40	45	45	
	Base de dades CRM	1	6.5	8	9	9		6.5	8	9	9	
	Base de dades de personal	5	4.55	7.2	7.2	5.4		22.75	36	36	27	
	Base de dades Navision Dynamics	5	5.2	6.4	7.2	6.3		26	32	36	31.5	
	Codi font aplicació pròpia d'inventari	1	0.35	4	4	2.5		0.35	4	4	2.5	
	Codi font aplicació pròpia d'alta i baixa d'usuaris	1	0.35	4	4	2.5		0.35	4	4	2.5	
	Codi font aplicació pròpia d'inventari de mòbils	1	0.35	4	4	2.5		0.35	4	4	2.5	
Xarxa												
	Línies RTB	1		0.05	0.05	3.75			0.05	0.05	3.75	
	Línies RDSI	10		0.35	0.40	6.8			3.5	4	68	
	Internet fibra òptica	10	4	6.4	4.80	7.2		40	64	48	72	
	LAN	10	4	6.4	4.8	7.2		40	64	48	72	
	VPN	10	4	6.4	4.2	5.4		40	64	42	54	
Serveis												
	Correu electrònic	7	4.5	6.75	6.75	8.1		31.5	47.25	47.25	56.7	
	Intranet	7	4	4.5	3.75	2.7		28	31.5	26.25	18.9	
	Emmagatzematge de dades	7	4.5	6.75	6.75	8.1		31.5	47.25	47.25	56.7	
	Teletreball	7	4	6	4.5	2.7		28	42	31.5	18.9	
Equipament auxiliar												
	Racks de servidors	1		0.1	0.1	1			0.1	0.1	1	
	Racks de comunicacions	1		0.1	0.1	1			0.1	0.1	1	
	SAI	1		0.75	2	8			0.75	2	8	
	Generador elèctric a gasoil	1		0.75	1.75	7			0.75	1.75	7	
	Climatització	1		0.75	2	9			0.75	2	9	
	Climatització de reserva	1		0.75	1.75	7			0.75	1.75	7	
	Control d'accés	1		1.5	1.75	3			1.5	1.75	3	
	Càmeres de vigilància	1		1.25	1	3			1.25	1	3	
	Sensors elèctrics i ambientals	1		0.25	1	4			0.25	1	4	
Personal												
	Usuaris interns	5		6.75	5	1			33.75	25	5	
	Administradors de sistemes	5		7.5	5	1			37.5	25	5	
	Programadors	5		7.5	4.5	0.6			37.5	22.5	3	
	Proveidors	4		1.5	1.5	0.7			6	6	2.8	

Taula 14: Nivell de risc.

Un cop calculat el risc, a la taula anterior podem veure remarcats tots els valors de risc que es trobem per sobre de valor establert per al risc Acceptable, que en el cas de la companyia és de 16 i per tant, seran els

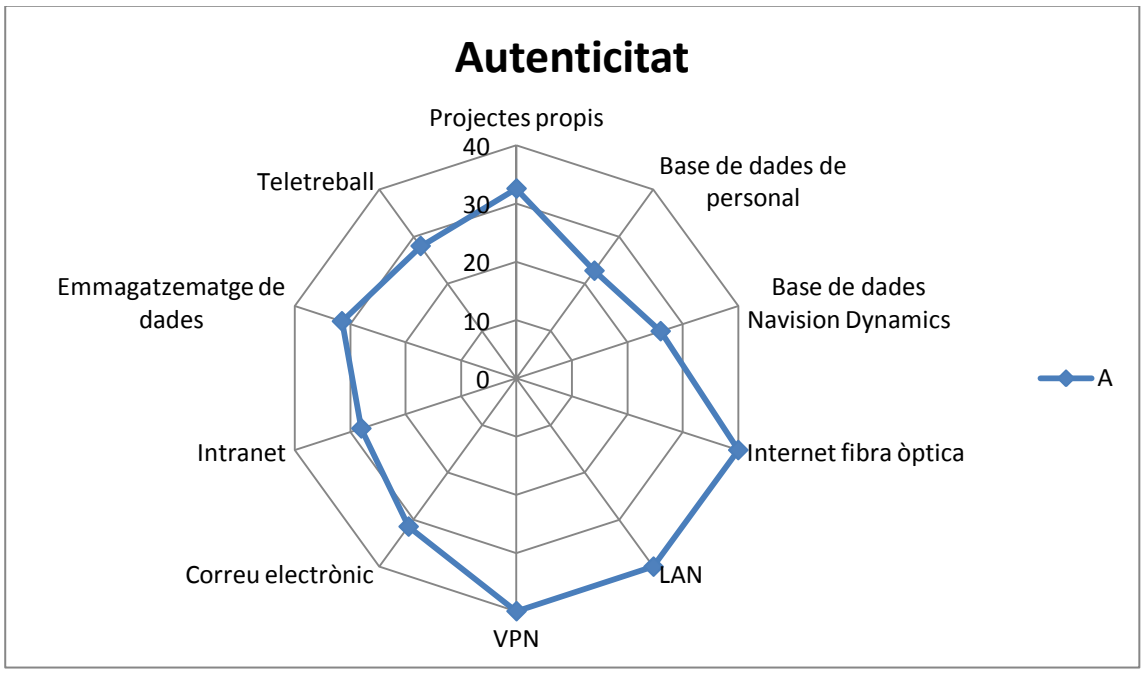
actius als quals s'hauran d'establir mesures per a reduir aquest risc i arribar a un risc residual.

A continuació podem veure una representació gràfica dels resultats obtinguts. Primer de tot tenim un gràfic de barres on podem veure els diferents actius, agrupats pel seu àmbit, amb el seu valor:

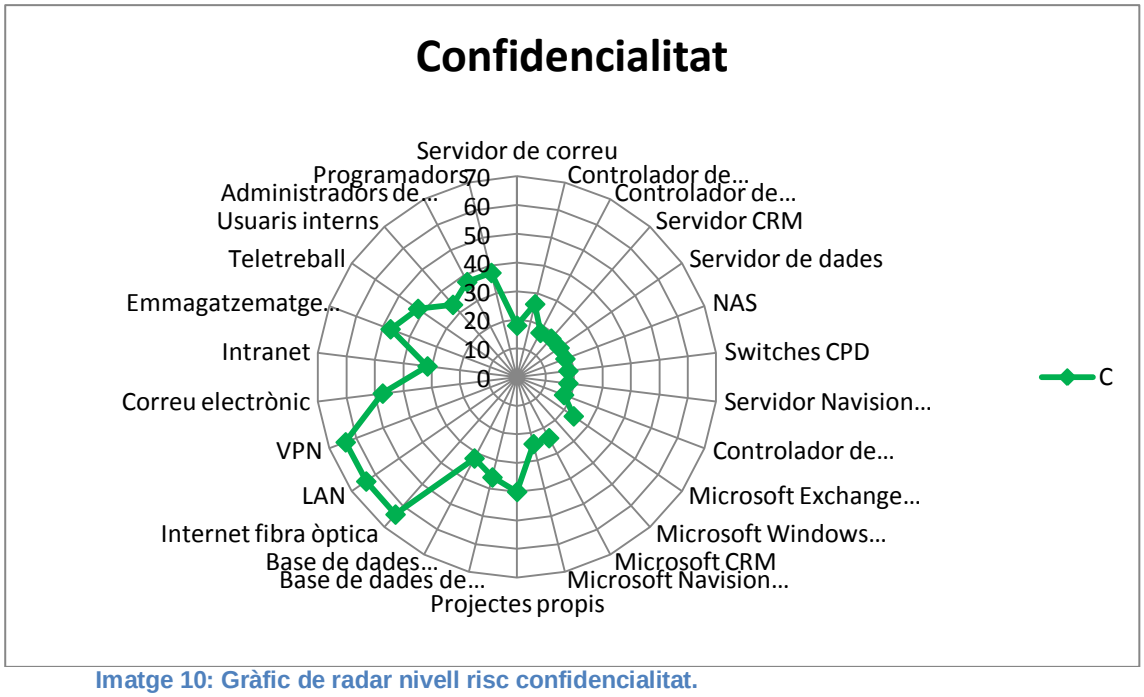


Imatge 8: Gràfic valor d'actius.

Tot seguit tenim un gràfic de radar per a cadascuna de les dimensions de seguretat (ACIDA) on podem veure la valoració del risc dels actius que superen el nivell de risc acceptable:

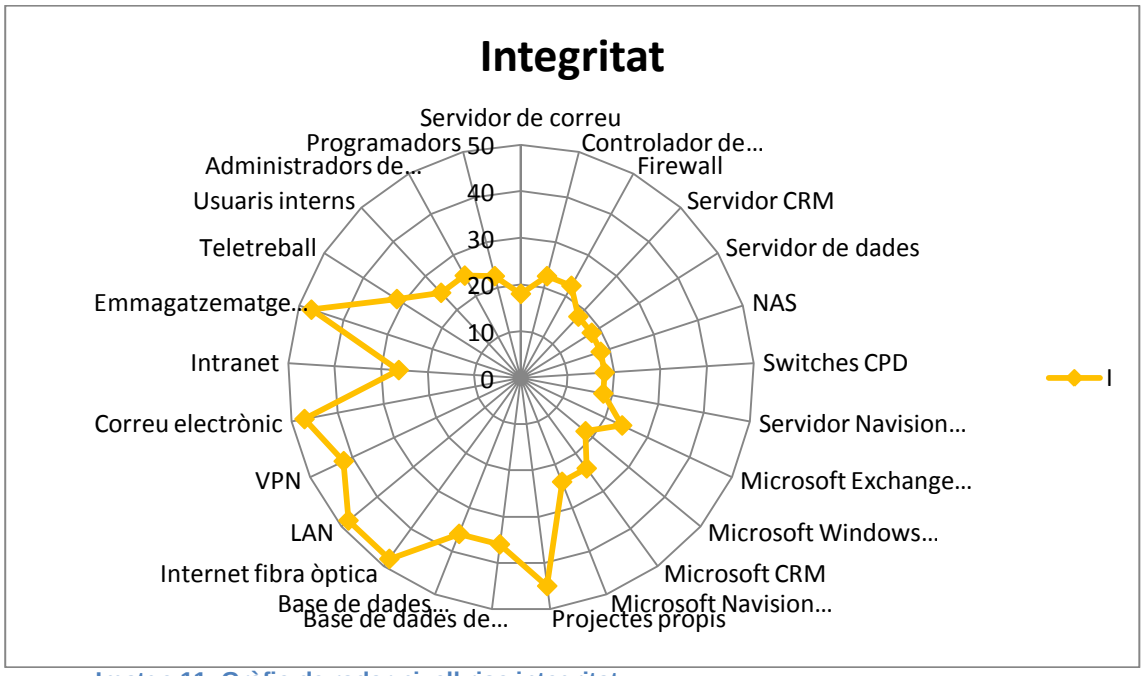


Imatge 9: Gràfic de radar nivell risc autenticitat.



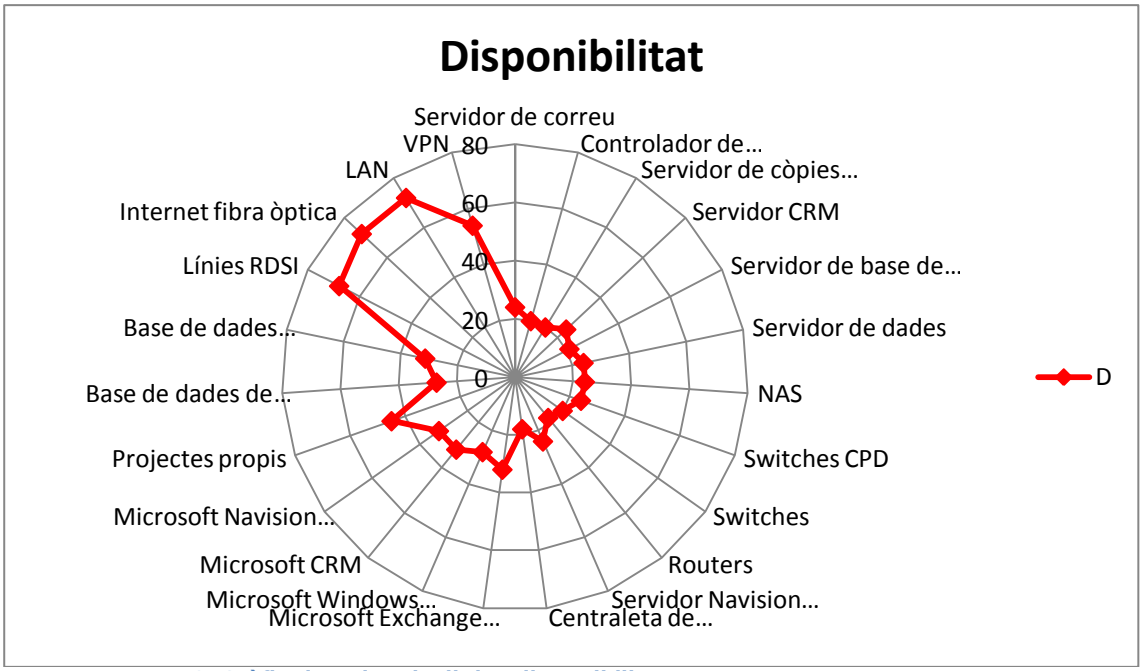
Imatge 10: Gràfic de radar nivell risc confidencialitat.

Com podem veure als gràfics anteriors, els actius que tenen el nivell de risc més alt a la dimensió de la confidencialitat i de l'autenticitat, són els relacionats amb l'àmbit de la xarxa (Internet fibra òptica, LAN, VPN).



Imatge 11: Gràfic de radar nivell risc integritat.

Com podem veure al gràfic anterior, els actius que tenen el nivell de risc més alt a la dimensió de la integritat, són els actius d'emmagatzematge de dades, correu electrònic, LAN i fibra òptica.



Imatge 12: Gràfic de radar nivell risc disponibilitat.

Com podem veure al gràfic anterior, els actius que tenen el nivell de risc més alt a la dimensió de la disponibilitat, també són els relacionats amb l'àmbit de la xarxa (Línies RDSI, Internet fibra òptica, LAN).

Per tant, la companyia ha de prendre atenció amb els controls dels actius nombrats anteriorment amb el nivell de risc major i treballar per a que el risc residual sigui el menor possible, ja que ens trobem amb nivells de risc molt alts.

La companyia es troba en un nivell de risc més elevat front a les amenaces provocades per la caiguda dels sistemes deguts a problemes físics, lògics o desastres (naturals o industrials), errors per part dels usuaris que puguin alterar la informació o malmetre els sistemes ja sigui per la instal·lació d'aplicacions no permeses o per desconeixement i problemes amb les comunicacions de la companyia.

4. Propostes de projectes

4.1 Introducció

Un cop realitzat l'anàlisi de riscos, s'han identificat els diferents actius més crítics de la companyia, els que suposen un impacte més greu i les vulnerabilitats més freqüents que poden ocórrer. Per tant, coneixem els actius que tenen un nivell de risc més alt, que serà sobre els que es realitzaran els següents projectes per millorar la seva situació de risc. Així com els dominis de la ISO/IEC 27002:2013 que es troben en el seu nivell inicial per tant de millorar la seguretat de la companyia.

4.2 Propostes

Es defineixen els següents projectes com a propostes de millora per als riscos de la companyia. Aquests projectes afectaran, com ja hem comentat, als actius crítics amb un nivell de risc per sobre del risc acceptable i als dominis de la ISO/IEC 27002:2013 amb un CMM L0.
Els projectes es redactaran amb un plantilla que contindrà la informació següent:

- Identificador del projecte.
- Nom del projecte.
- Descripció.
- Objectius.
- Els actius de la companyia afectats.
- Dominis ISO/IEC 27002:2013 afectats.
- Riscos mitigats.
- Durada.
- Recursos necessaris (personal i econòmic).
- Període de consecució.

Tenim les següents propostes de projectes:

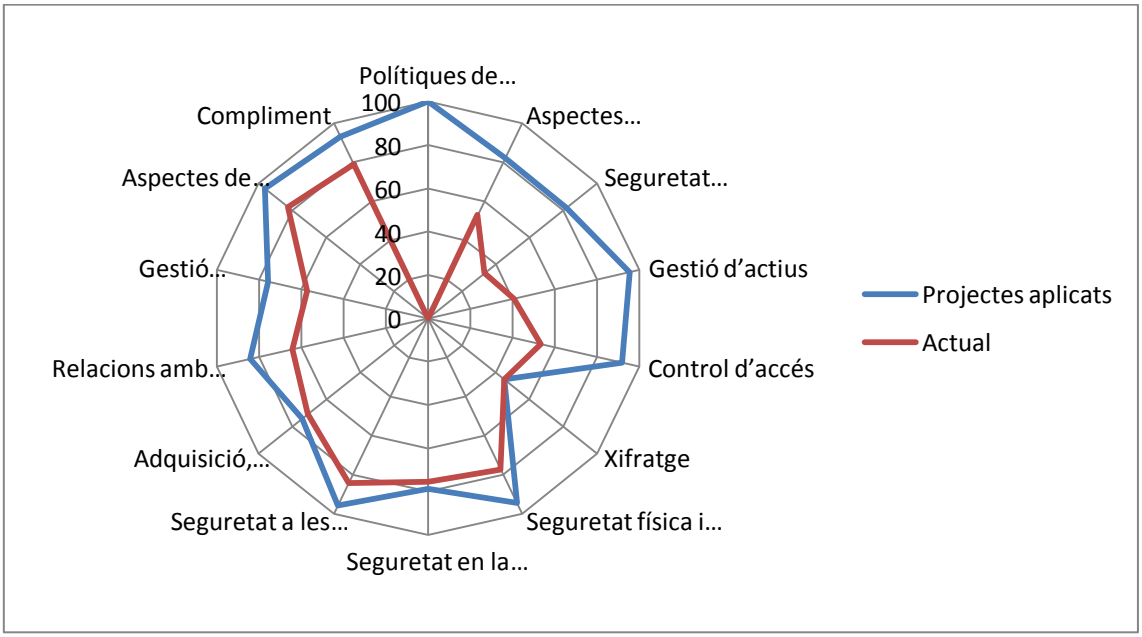
- PRO-001: Establiment de la política de seguretat.
- PRO-002: Document de seguretat per a les noves contractacions.
- PRO-003: Document per establir el protocol de classificació de la informació.

- PRO-004: Implantació d'un MDM.
- PRO-005: Procediment per a la documentació de TI.
- PRO-006: Política de seguretat per a la instal·lació de software.
- PRO-007: Seguretat del Hardware i serveis crítics.
- PRO-008: Document de control de les còpies de seguretat.
- PRO-009: Continuïtat de les comunicacions externes de la companyia.
- PRO-010: Pla de formació als usuaris en seguretat de la informació.

A l'annex 9 podem veure amb detall els diferents projectes proposats a la companyia.

4.3 Resultats

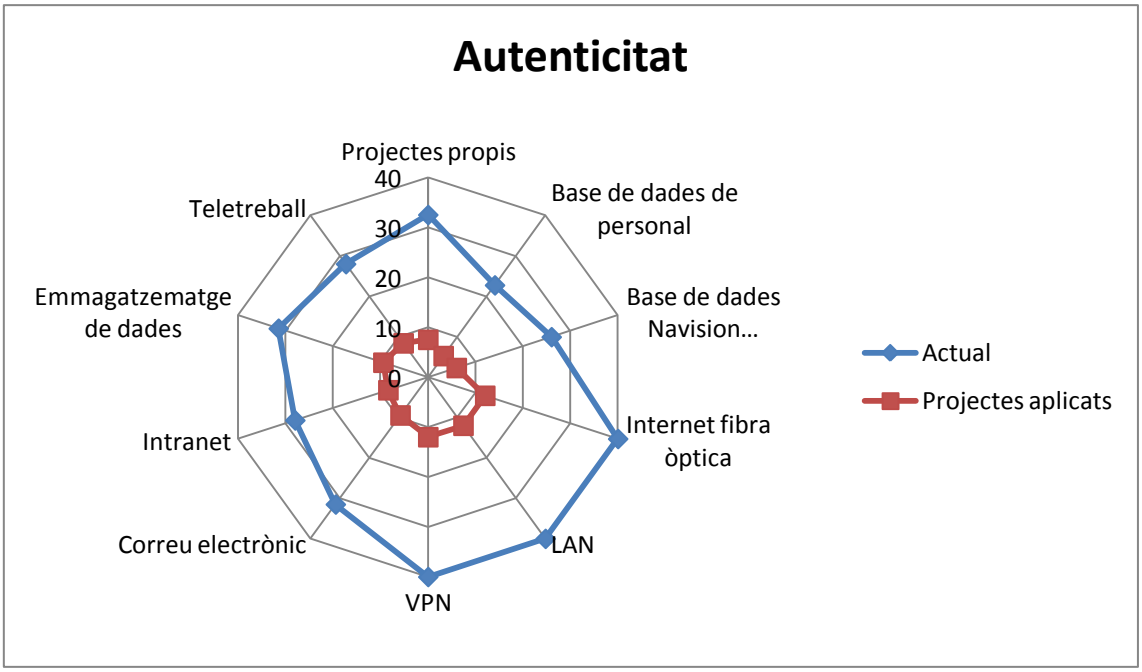
Un cop implementats els projectes anteriors, s'obtindria una millora al nivell de risc dels actius i una maduració del CMM dels diferents controls de la norma ISO/IEC 27002:2013. A l'annex 10 podem veure la taula comparativa amb els controls ISO/IEC 27002:2013 i el seus valors CMM actualitzats un cop aplicats els projectes. Tot seguit podem veure els resultats representats al següent gràfic de radar per dominis de la ISO/IEC 27002:2013.



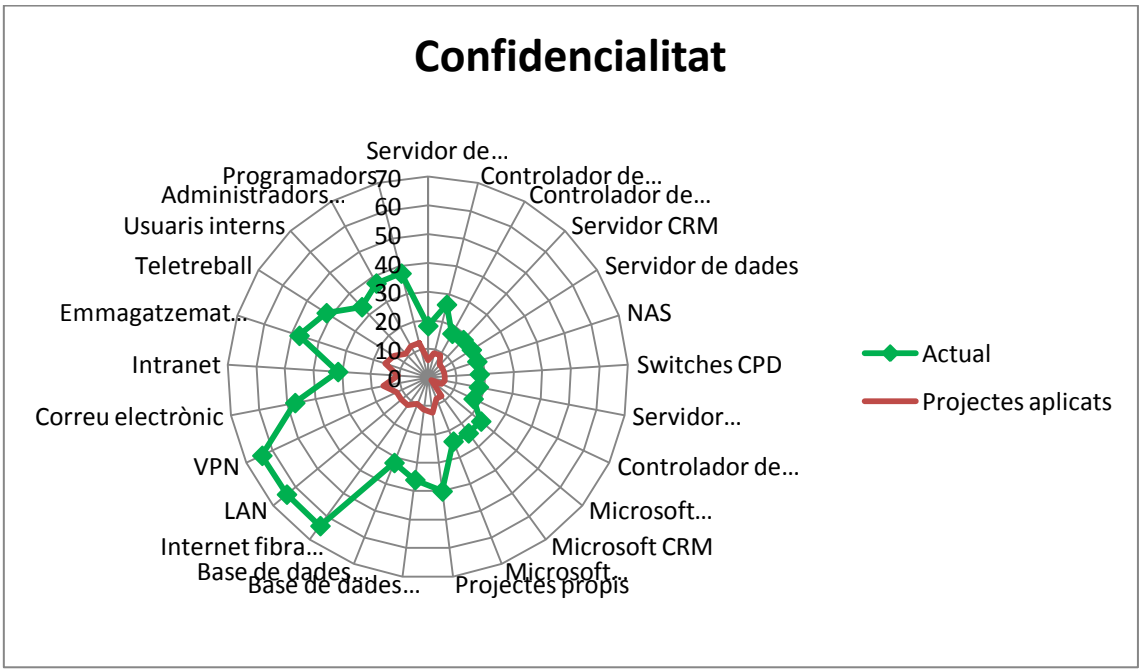
Imatge 13: Diagrama de radar amb la comparativa dels valors CMM dels controls ISO 27002 un cop aplicats els projectes.

Com podem veure al gràfic anterior, un cop aplicats els projectes proposats, ha millorat l'estat de maduresa de pràcticament tots els dominis de la ISO/IEC 27002:2013, a excepció del xifratge degut a que no s'ha realitzat la proposta de cap projecte que afecti a aquest domini que no és crític per a la nostra companyia. Els dominis que han millorat substancialment són el relatiu a la política de seguretat degut a que s'ha realitzat la seva implementació amb l'aprovació de la direcció, el de gestió d'actius gràcies a la implementació de l'MDM, el protocol de classificació de la informació i el domini de seguretat lligada als recursos humans degut a l'aplicació del projecte relacionat amb la documentació de seguretat per a les noves contractacions i al pla de formació als usuaris en seguretat de la informació.

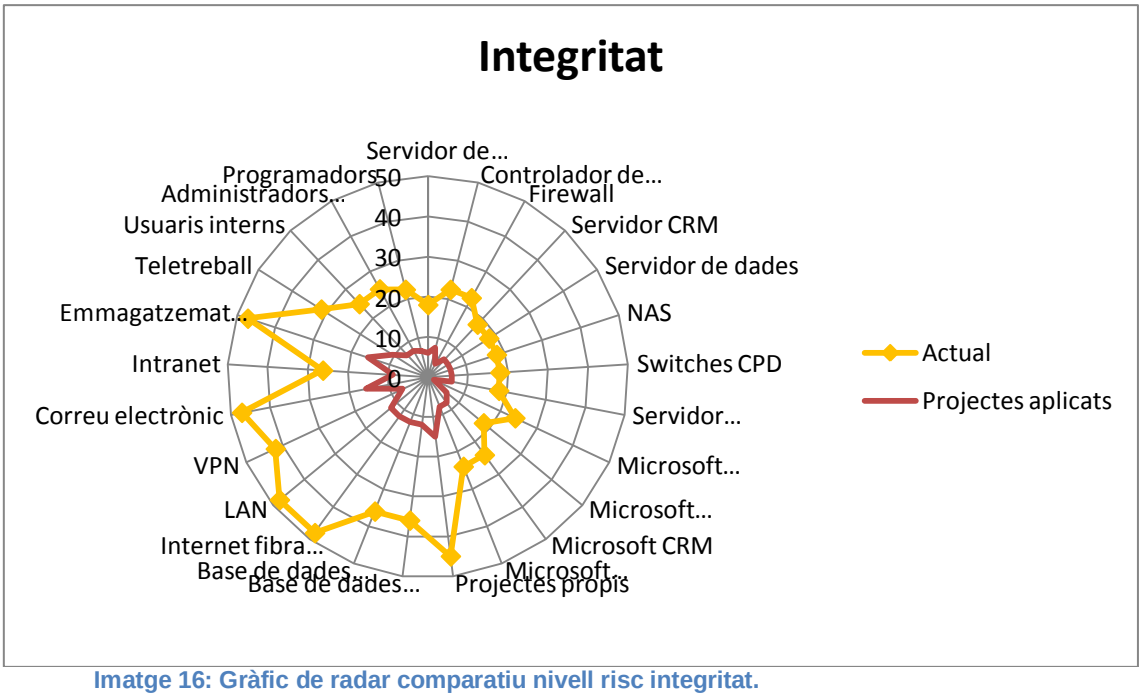
A l'annex 11 podem veure la taula comparativa de l'impacte potencial abans i després d'aplicar els projectes, la modificació d'aquest impacte potencial es deu a una reducció a l'impacte màxim d'amenaça que pot rebre l'actiu després d'haver implementat els projectes proposats. Amb la informació de la taula citada anteriorment, s'han calculat els diferents nivells de risc per a cada actiu. Aquesta taula comparativa del nivell de risc abans i després d'aplicar els projectes, la podem veure a l'annex 12. Els següents gràfics de radar representen l'evolució del nivell de risc per a cada dimensió ACIDA dels actius que superaven el nivell de risc acceptable de la companyia abans d'aplicar els projectes. Com es pot apreciar, tots els actius milloren el seu nivell de risc a totes les dimensions, encara que a la dimensió de disponibilitat trobem actius relacionats amb la xarxa i els serveis, que un cop reduït el seu nivell de risc encara superen el nivell de risc acceptable per la companyia necessitant de futures actuacions que permetin reduir el risc en aquests actius:



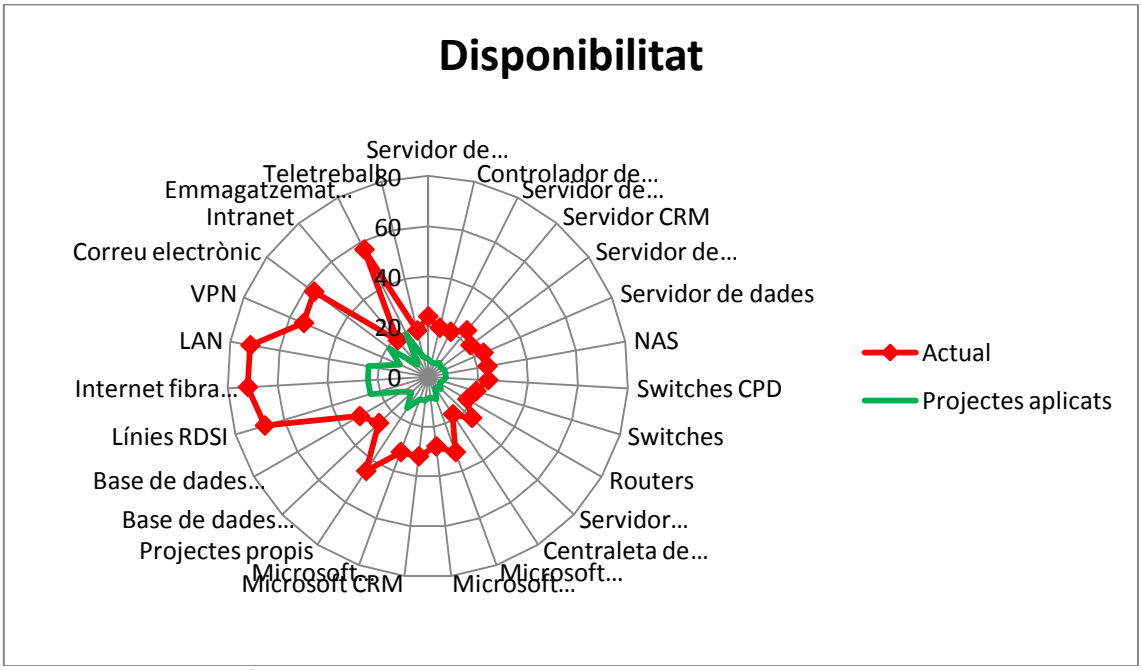
Imatge 14: Gràfic de radar comparatiu nivell risc autenticitat.



Imatge 15: Gràfic de radar comparatiu nivell risc confidencialitat.



Imatge 16: Gràfic de radar comparatiu nivell risc integritat.



Imatge 17: Gràfic de radar comparatiu nivell risc disponibilitat.

5. Auditoria de Compliment

5.1 Introducció

Un cop aplicades les diferents propostes de projectes, per millorar la seguretat de la informació a la companyia, ens trobem al punt de dur a terme una auditoria interna per comprovar l'estat actual de compliment dels diferents controls de la norma ISO/IEC 27002:2013 i de l'estat de maduresa dels mateixos i així conèixer en quin punt es troba la companyia front a una certificació de la norma ISO/IEC 27001.

Tot seguit es documentaran les diferents fases del procés d'auditoria de compliment i un cop comprovada la maduresa dels controls ISO/IEC 27002:2013 s'informarà de les no conformitats trobades per tant de solucionar-les i poder obtindre la certificació de la norma sense problemes.

Per finalitzar l'auditoria de compliment veurem els resultats obtinguts comparant-los amb l'estat de maduresa dels controls al inici del projecte.

5.2 Auditoria

Es realitzarà una auditoria interna o de primera part que avaluarà l'estat de la seguretat de la informació de la companyia un cop aplicades les propostes de projectes. Aquesta auditoria constarà de les següents fases:

- Pla d'auditoria.
    - Informació general.
    - Procediment i control de proves.
- Execució de l'auditoria.
- Informe de l'auditoria.
    - Resum executiu.
    - Metodologia emprada.
    - Llista detallada de constatacions.

5.2.1 Pla d'auditoria

El pla d'auditoria consta dels següents apartats:

- Informació general:
  - Objectiu.
  - Abast.
  - Visió general del sistema.
  - Documentació de referència.
- Procediment i control de proves.

5.2.2 Execució de l'auditoria

Un cop s'ha establer el pla d'auditoria, es procedirà amb l'execució de la mateixa. En aquest punt es recollirà i es revisarà tota la documentació necessària per a l'avaluació del sistema, es realitzaran les entrevistes amb els responsables dels departaments afectats, s'executaran les diferents proves tècniques, com el control del backup... i es realitzaran les visites necessàries per verificar els aspectes de seguretat física.

Un cop recopilada tota la informació anterior, es procedirà amb l'anàlisi de la informació on s'avaluaran els diferents controls amb la informació aconseguida en els processos anteriors d'aquesta fase. Al finalitzar aquest anàlisis es coneixeran les no conformitats que haurà de fer front la companyia.

5.2.3 Informe d'auditoria

L'informe d'auditoria constarà de les següents parts:

- Resum executiu: S'adjuntarà un resum de les troballes de l'auditoria amb les possibles millores per al sistema de seguretat de la informació. Aquest resum estarà orientat a la direcció i realitzarà una petita introducció a la metodologia emprada.
- Metodologia emprada: S'indicaran les normes i mètodes utilitzats per a la realització de l'auditoria de compliment.
- Llista detallada de constatacions: Al final del procés d'auditoria de compliment, es podran redactar les diferents evidències trobades

que no compleixen amb la norma ISO/IEC 27002:2013 i es procedirà amb la redacció de les no conformitats.

5.3 Avaluació de la maduresa

A l'informe d'auditoria adjunt a l'annex 13 es pot veure la taula de compliment dels 114 controls de la norma ISO/IEC 27002:2013 i el seu estat de maduresa seguint el Model de Maduresa de la Capacitat (CMM).

5.4 No conformitats

Un cop realitzada la taula de compliment dels 114 controls de la norma ISO/IEC 27002:2013 amb l'estat de maduresa, podem obrir les no conformitats que han sortit de l'auditoria d'aplicabilitat de tots els controls que no compleixen amb la norma.

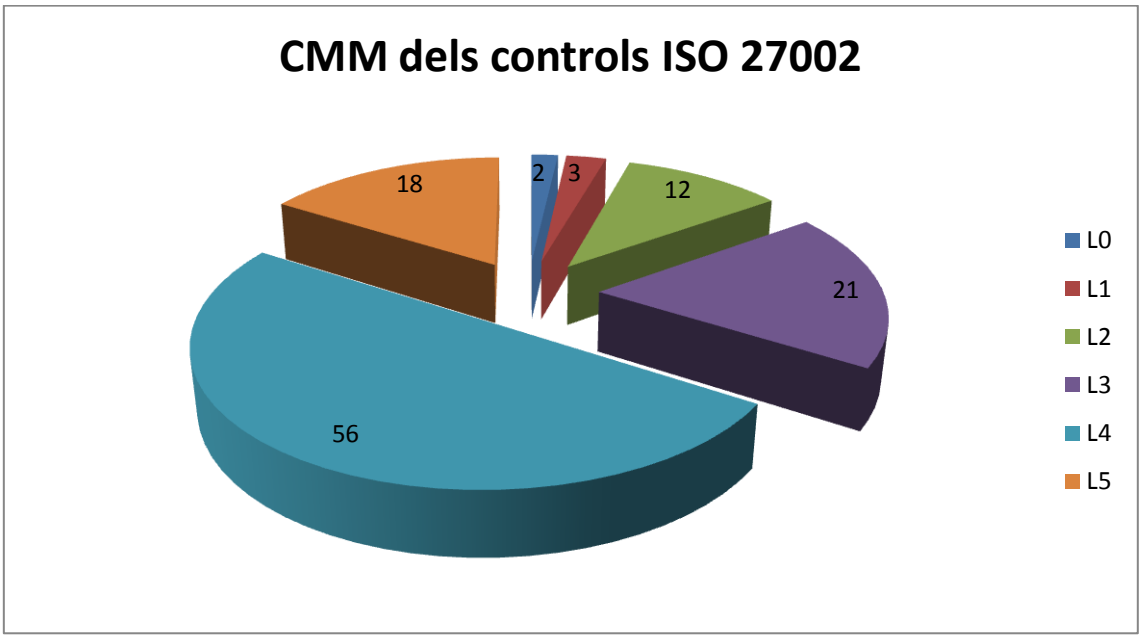
Les no conformitats es redactaran amb un plantilla que contindrà la informació següent:

- Identificador de la no conformitat.
- Data d'obertura.
- Data finalització
- Descripció.
- Tipus (major o menor).
- Domini de la norma ISO/IEC 27002:2013 afectat.
- Els controls afectats.
- Acció correctora.
- Responsable assignat.

Les no conformitats les podem veure detallades a l'informe d'auditoria adjunt a l'annex 13.

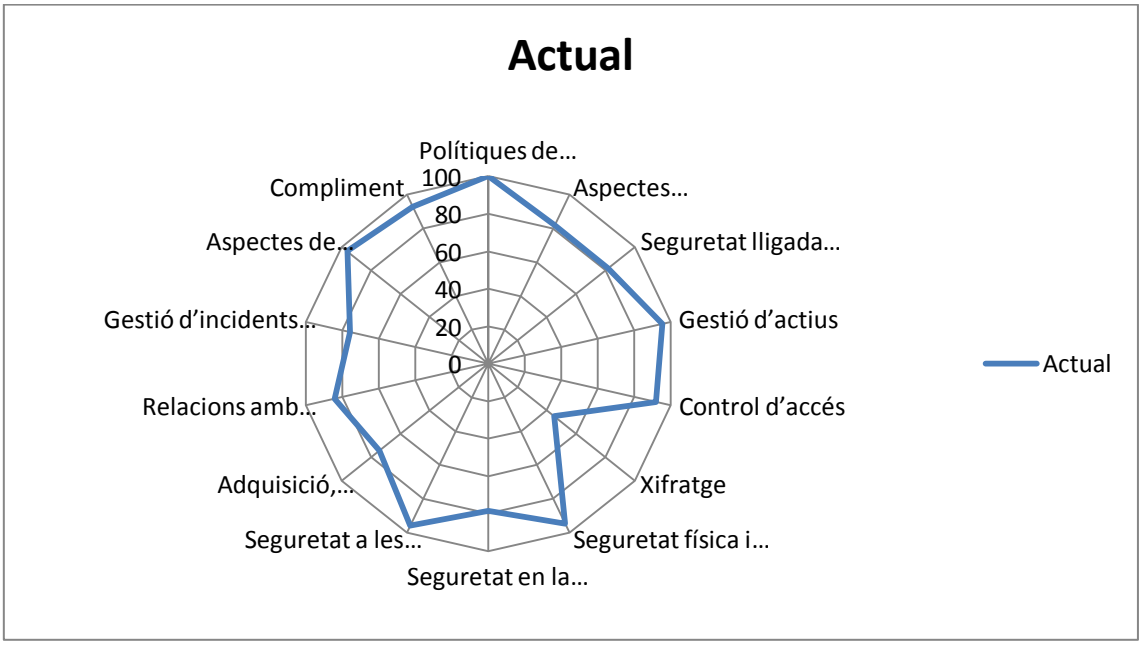
5.5 Resultats

Un cop realitzada l'auditoria de compliment, podem representar gràficament els resultats de la taula de compliment dels 114 controls de la norma ISO/IEC 27002:2013 amb el seu nivell de maduresa. El gràfic següent ens mostra la distribució per nivell de maduresa:



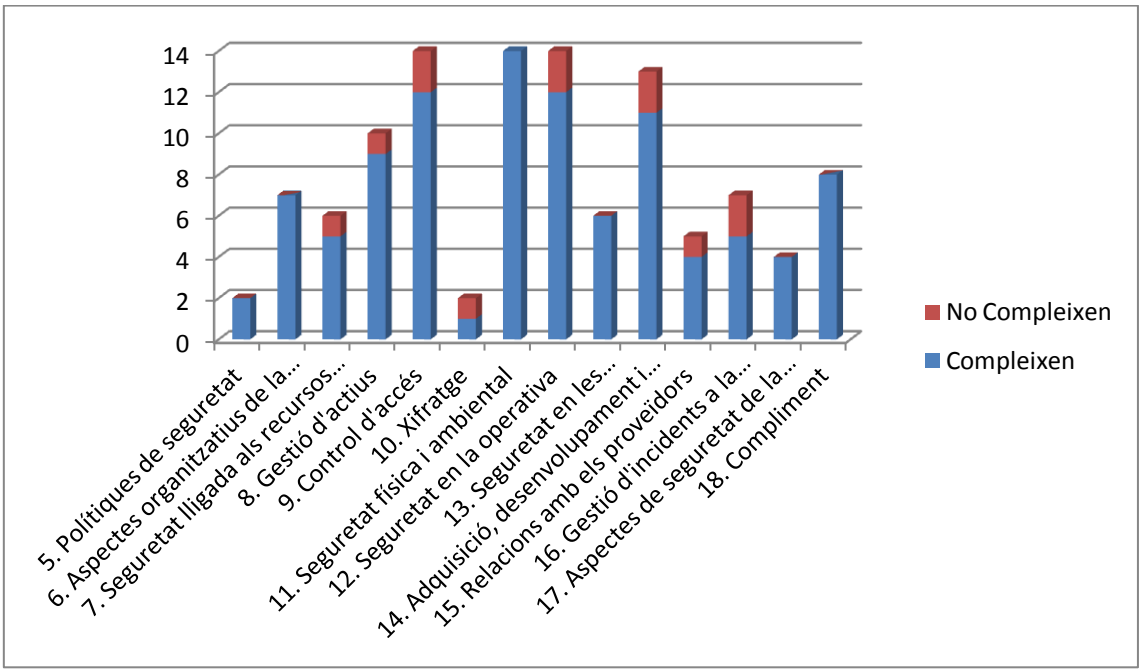
Imatge 18: Gràfic amb els valors CMM dels controls ISO 27002 després de l'auditoria de compliment.

Tot seguit podem veure l'estat del nivell CMM dels diferents dominis de la norma ISO/IEC 27002:2013 representats al següent gràfic de radar:



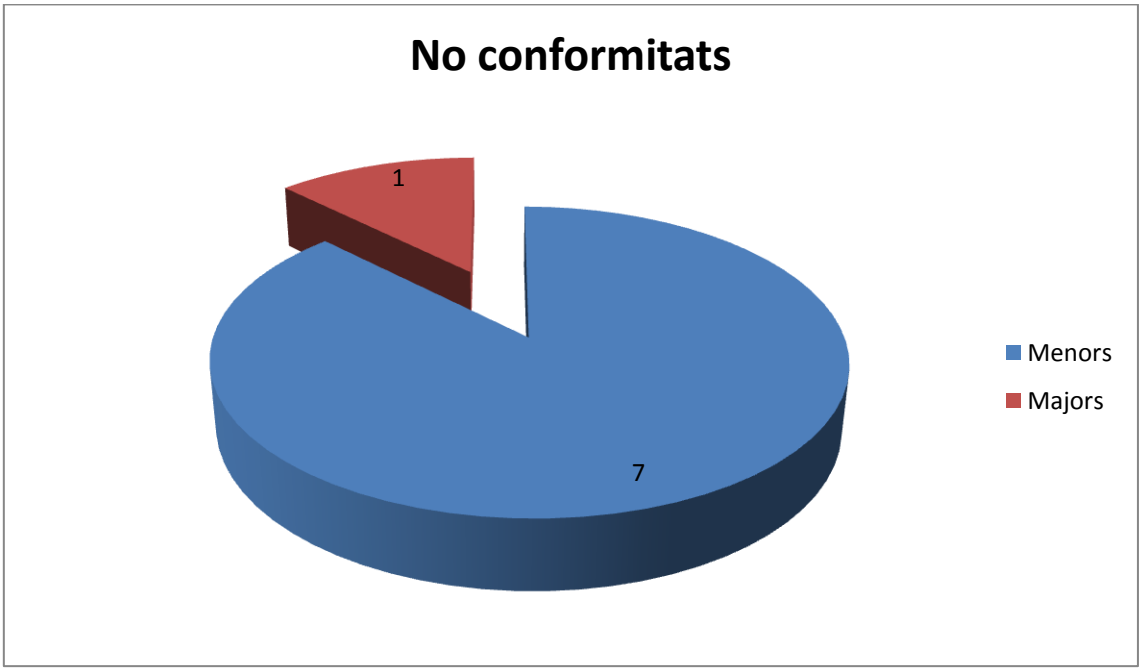
Imatge 19: Diagrama de radar amb els valors CMM dels controls ISO 27002 després de l'auditoria de compliment.

A continuació, podem veure un gràfic on es mostren els controls que compleixen o no compleixen amb la normativa per a cada domini:



Imatge 20: Compliment dels controls per dominis ISO/IEC 27002:2013.

Per últim tenim un gràfic on podem veure el total de no conformitats agrupades segons el seu tipus (majors o menors):



Imatge 21: Total de no conformitats per tipus.

Amb la informació anterior, veiem que després de realitzar l'auditoria de compliment, s'han trobat no conformitats en 8 dels 14 dominis , afectant a 12 dels 114 controls (el 10,53%) de la norma ISO/IEC 27002:2013, de

les quals només s'ha trobat una no conformitat major que s'haurà de resoldre de manera més immediata i set no conformitats de tipus menor que s'hauran de solucionar abans de la següent auditoria.

Un cop comparat l'estat de la companyia amb el començament del SGSI, podem dir que els controls han millorat molt el seu estat de maduresa, ja que ara només tenim 2 controls en un estat inexistent mentre que al inici del projecte teníem 11 i la majoria dels controls es troben per sobre del 90% d'efectivitat.

Si ens fixem en els dominis, les polítiques de seguretat de la companyia han passat a tindre una efectivitat del 100%, la gestió d'actius, control d'accés, seguretat física i ambiental, seguretat en les telecomunicacions, aspectes de seguretat de la informació a la gestió de la continuïtat del negoci i compliment es troben per sobre del 90% d'efectivitat, aspectes organitzatius de la seguretat de la informació, seguretat lligada als recursos humans, seguretat en l'operativa, relacions amb proveïdors i gestió d'incidents a la seguretat de la informació estan per sobre del 75%, adquisició, desenvolupament i manteniment dels sistemes d'informació es troba al 74,23% i per últim tenim que el domini amb una maduresa més baixa és el de xifratge que es troba al 45% igual que es trobava a l'estat inicial, degut a que aquest domini no ha rebut cap tipus de proposta de projecte.

6. Conclusions

La principal millora que obté una companyia amb l'aplicació d'un SGSI, la tenim amb la reducció dels riscos de que una amenaça es materialitzi afectant als actius de la companyia, produint una pèrdua d'informació i afectant a la continuïtat del negoci aportant un cost econòmic molt elevat. També ens donarà una millor imatge front a clients i ens permetrà obtenir una certificació de seguretat.

Els objectius principals del SGSI s'han complert a excepció de la garantia de compliment de la legislació que aplica a la companyia, el departament jurídic en la companyia serà l'encarregat de documentar aquestes necessitats i un cop realitzat l'informe s'adjuntarà al SGSI.

Per a la realització del SGSI se'ns ha proporcionat una planificació establerta en cinc fases diferenciades que s'ha pogut seguir sense incidents, amb una metodologia vàlida per a la realització de les diferents fases.

Un cop realitzat l'SGSI, implantat i realitzada l'auditoria de compliment, ens quedarà pendent l'informe de compliment de la legislació vigent que afecta a la companyia, resoldre les diferents no conformitats obertes i realitzar un seguiment de les mateixes i futures evolucions del SGSI.

7. Glossari

- **ACIDA:** Dimensions de seguretat (Autenticitat, Confidencialitat, Integritat, Disponibilitat i Auditabilitat).
- **Actiu:** En relació amb la seguretat de la informació, es refereix a qualsevol informació o element relacionat amb el tractament de la mateixa (sistemes, suports, edificis, persones...) que tingui valor per a l'organització.
- **Amenaça:** Causa potencial d'un incident no desitjat, que pot provocar danys a un sistema o a l'organització.
- **CEO:** Chief Executive Officer. Director exectiu.
- **CMM:** Capability Maturity Model. Model de maduresa de les capacitats.
- **CPD:** Centre de processament de dades.
- **CRM:** Customer Relationship Management. Gestor de relació amb clients.
- **ERP:** Enterprise Resource Planning. Planificació de recursos empresarials.
- **Firewall:** Un firewall és un sistema que protegeix a un ordinador o a una xarxa d'ordinadors contra intrusions provinents de xarxes de tercers (generalment des d'Internet).
- **IEC:** International Electrotechnical Commission. Organització Internacional que publica estàndards relacionats amb tot tipus de tecnologies elèctriques i electròniques.
- **ISO:** Organització Internacional de Normalització, amb seu a Ginebra (Suïssa). És una agrupació d'entitats nacionals de normalització amb l'objectiu d'establir, promocionar i gestionar estàndards (normes).
- **Impacte:** El cost per a l'empresa d'un incident, que pot o no ésser mesurat en termes estrictament financers.
- **LAN:** Local Area Network. Xarxa d'àrea local.
- **LOPD:** Llei Orgànica 15/1999 del 13 de desembre de Protecció de Dades de Caràcter Personal.

- **MAGERIT:** És una metodologia d'anàlisi i gestió de riscos dels Sistemes de Informació elaborada pel Consell Superior d' Administració Electrònica per a minimitzar els riscos de la implantació i ús de les Tecnologies de la Informació, enfocada a les Administracions Públiques.
- **MDM:** Mobile Device Management. Administració dels dispositius mòbils.
- **NAS:** Network Attached Storage. Sistema d'emmagatzematge connectat a la xarxa.
- **No conformitat:** Incompliment d'un requisit.
- **RDSI:** Xarxa Digital de Serveis Integrats.
- **SGSI:** Sistema de Gestió de la Seguretat de la Informació. Segons [ISO/IEC 27001:2005]: la part d'un sistema global de gestió que, basat en l'anàlisi de riscos, estableix, implementa, opera, monitora, revisa, manté i millora la seguretat de la informació.
- **VLAN:** Virtual Local Area Network. Xarxa d'àrea local virtual.
- **VPN:** Virtual Private Network. Xarxa privada virtual.
- **Vulnerabilitat:** Debilitat d'un actiu o control que pot ser explotada per una o més amenaces.

8. Bibliografia

1. El portal de ISO 27001 en Español. [Internet] Disponible a: http://iso27000.es/ . Copyright © 2012.
2. Lista de documentación obligatoria requerida por ISO/IEC 27001 (Revisión 2013). 27001 Academy. [Internet]. Disponible a: http://cdn2.iso27001standard.com/Checklist_of_Mandatory_Documentation_Required_by_ISO_27001_2013_ES.pdf . Copyright © 2013 27001 Academy.
3. ISO 27001: Auditorias internas del SGSI. PMG-SSI. [Internet]. 2014. Disponible a: http://www.pmg-ssi.com/2014/12/iso-27001-auditorias-internas-del-sgsi/ . Copyright © 2015 PMG-SSI.
4. ISO 27001: Revisión por la dirección y mejora del SGSI. PMG-SSI. [Internet]. 2014. Disponible a: http://www.pmg-ssi.com/2014/12/iso-27001-revision-por-la-direccion-y-mejora-del-sgsi/ . Copyright © 2015 PMG-SSI.
5. ¿Cómo hacer la revisión por la dirección? 5 Consultores. [Internet]. 2013. Disponible a: http://www.5consultores.com/como-hacer-la-revision-por-la-direccion/ . Aquesta obra es publica sota una llicencia Creative Commons.
6. Revisión por la dirección. eGAM. [Internet]. Disponible a: http://www.egambpm.com/wiki/index.php?title=Revisi%C3%B3n_por_la_Direcci%C3%B3n . Suposem que té Copyright ja que l'autor no ens ho indica.
7. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. [Internet]. 2012. Disponible a: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf . Copyright © Ministerio de Hacienda y Administraciones Públicas.
8. Capítulo 3.2 Lección 12: Metodología MAGERIT. UNAD. [Internet]. Disponible a: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/32_leccin_12_metodologa_magerit.html . Suposem que té Copyright ja que l'autor no ens ho indica.
9. Poveda, J.M. Módulo 8: Análisis y valoración de los riesgos. Metodologías. ISO 27001. [Internet]. Disponible a: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf . Aquesta obra es publica sota una llicencia Creative Commons.

9. Annexos

9.1. Annex 1: 114 Controls de la ISO/IEC 27002:2013.

Tot seguit tenim els 114 controls de la ISO/IEC 27002:2013 valorats mitjançant el Model de Maduresa de la Capacitat (CMM).

Dominis	Objectius de control	Controls	CMM	Observacions
5. Polítiques de Seguretat				
	5.1. Directrius de la Direcció en seguretat de la informació			
		5.1.1. Conjunt de polítiques per a la seguretat de la informació.	L0	No existeix cap política per a la seguretat de la informació aprovada per la direcció, publicada i comunicada.
		5.1.2. Revisió de les polítiques per a la seguretat de la informació.	L0	No es disposa de cap política a verificar.
6. Aspectes Organitzatius de la seguretat de la informació				
	6.1. Organització Interna.			
		6.1.1. Assignació de responsabilitats per a la seguretat de la informació.	L2	La companyia disposa de personal assignat a les tasques de seguretat encara que no existeix un document on apareguin.
		6.1.2. Segregació de taques.	L3	En quant a l'ús dels actius de l'organització, aquests es troben controlats tant pel departament d'administració com d'infraestructura de la informació.
		6.1.3. Contacte amb les autoritats.	L3	
		6.1.4. Contacte amb els grups d'interès especial.	L2	Els responsables de seguretat del departament d'infraestructura de la informació revisen tota la informació de seguretat tant amb externs com amb foros.
		6.1.5. Seguretat de la informació a la gestió	L5	La informació dels diferents projectes

Dominis	Objectius de control	Controls	CMM	Observacions
		de projectes.		de la companyia és accessible amb permisos assignats als diferents nivells d'usuari, es troba documentat i l'estructura de carpetes i els permisos es donen d'alta amb una utilitat informàtica pròpia.
	6.2. Dispositius per a la mobilitat i el teletreball.			
		6.2.1. Política d'ús de dispositius per a la mobilitat.	L1	Existeix una política de seguretat en quant a actualitzacions d'antivirus... d'equips que es troben fora de la companyia. Però no es disposa de cap MDM per a un control exhaustiu dels dispositius mòbils, ni polítiques de xifratge de dades o USB quan l'equip es troba fora de la companyia.
		6.2.2. Teletreball.	L2	Les tasques de teletreball són temporals i als usuaris només se'ls permet accedir al seu equip de treball de la companyia amb el software de connexió VPN proporcionat pel departament d'infraestructures de la informació. Els usuaris VPN es donen d'alta pels membres del departament d'infraestructura de la informació. No es disposa de documentació on s'indiqui els procediment a seguir.
7. Seguretat lligada als recursos humans.				
	7.1. Abans de la contractació.			
		7.1.1. Investigació d'antecedents.	L2	Realitzat pel departament de RRHH, encara que

Dominis	Objectius de control	Controls	CMM	Observacions
				no existeix documentació.
		7.1.2. Termes i condicions de contractació.	L2	Un cop signat el contracte, tots els empleats reben una copia del document del reglament de compliment normatiu, encara que falta la documentació de seguretat de la informació.
	7.2. Durant la contractació.			
		7.2.1. Responsabilitats de gestió.	L0	No existeix cap normativa de seguretat de la informació.
		7.2.2. Conscienciació, educació i capacitació en seguretat de la informació.	L0	Actualment no s'estan realitzant.
		7.2.3. Procés disciplinari.	L0	No existeix aquest procés.
	7.3. Cessament o canvi de lloc de treball.			
		7.3.1. Cessament o canvi de lloc de treball.	L2	La devolució d'actius dels empleats i baixa o bloqueig de comptes d'usuari es controla conjuntament pel departament de RRHH, Administració i infraestructura de la informació.
8. Gestió d'actius.				
	8.1. Responsabilitat sobre els actius.			
		8.1.1. Inventari d'actius.	L4	L'inventari d'actius es controla amb una utilitat pròpia, els usuaris tenen accés per veure els actius que tenen assignats, en cas d'error poden enviar una incidència per solvatar el problema. El programa propi té informació de l'actiu que comparteix amb l'ERP de la companyia.
		8.1.2. Propietat dels actius.	L4	Els actius es troben assignats a

Dominis	Objectius de control	Controls	CMM	Observacions
				usuaris, departaments i empreses.
		8.1.3. Ús acceptable dels actius.	L3	Els actius de recursos de la informació és troben identificats, encara que no tots estan documentats, com per exemple els històrics de dades.
		8.1.4. Devolució d'actius.	L3	La devolució d'actius es realitza en el moment en que es formalitza la baixa del contracte laboral amb la companyia.
	8.2. Classificació de la informació.			
		8.2.1. Directrius de classificació.	L0	No es disposa d'un sistema de classificació de la informació.
		8.2.2. Etiquetatge i manipulació de la informació.	L1	L'etiquetatge no indica el nivell de classificació al ser aquest inexistent.
		8.2.3. Manipulació d'actius.	L1	El procediment de manipulació d'actius no varia en funció de la informació continguda.
	8.3. Maneig dels suports d'emmagatzematge			
		8.3.1. Gestió de suports extraïbles.	L2	Els medis informàtics extraïbles destinats a les còpies de seguretat es porten a una ubicació externa amb un servei ofert per un tercer complint amb les mesures de seguretat. Però, els dispositius extraïbles USB no es troben controlats per cap política de seguretat existent.
		8.3.2. Eliminació de suports.	L1	La informació sensible continguda en dispositius informàtics és eliminada al final de la seva vida útil, però no es segueix cap procediment documentat.
		8.3.3. Suports físics	L1	No existeix cap

Dominis	Objectius de control	Controls	CMM	Observacions
		en transit.		procediment de xifratge d'informació per a dispositius extraïbles en transit.
9. Control d'accés.				
	9.1. Requisits de negoci per al control d'accessos.			
		9.1.1. Política de control d'accessos.	L2	Existeix un procediment no documentat en quant a la política de control d'accés.
		9.1.2. Control d'accés a les xarxes i serveis associats.	L4	Tots els usuaris tenen disponibles les utilitats per a les quals se'ls i ha donat accés.
	9.2. Gestió d'accés d'usuari.			
		9.2.1. Gestió d'altes/baixes al registre d'usuaris.	L5	Existeix una utilitat pròpia enllaçada amb la utilitat d'incidències per sol·licitar tant les altes com les baixes d'usuaris des de RRHH al departament d'infraestructura de la informació.
		9.2.2. Gestió dels drets d'accés assignats a usuaris.	L2	La sol·licitud de drets d'accés a usuaris es canalitza pels seus responsables mitjançant una incidència, encara que no existeix cap document que ho indiqui.
		9.2.3. Gestió dels drets d'accés amb privilegis especials.	L2	Aquests tipus d'accessos es sol·liciten mitjançant incidència des de el responsable del departament afectat.
		9.2.4. Gestió d'informació confidencial d'autenticació d'usuaris.	L4	Tota la informació confidencial que tingui l'usuari per a la seva autenticació vindrà donada per la utilitat d'altes i baixes al personal indicat.
		9.2.5. Revisió dels drets d'accés dels usuaris.	L2	Es realitzen sol·licituds de baixa d'accessos a BBDD per diferents responsables de l'organització,

Dominis	Objectius de control	Controls	CMM	Observacions
				encara que no existeix cap procediment de revisió.
		9.2.6. Retirada o adaptació dels drets d'accés.	L4	Es realitzen les baixes d'usuari a petició del departament de RRHH cap al departament d'infraestructura de la informació mitjançant la utilitat pròpia d'altes i baixes.
	9.3. Responsabilitats de l'usuari.			
		9.3.1. Ús d'informació confidencial per a l'autenticació.	L1	No es disposa de cap document que indiqui a l'usuari les seves responsabilitats, encara que se li indiquen.
	9.4. Control d'accés a sistemes i aplicacions.			
		9.4.1. Restricció de l'accés a la informació	L3	L'accés a les dades es troba restringit en funció del nivell o necessitat de cada usuari.
		9.4.2. Procediments segurs d'inici de sessió.	L3	Totes les aplicacions i dades de la companyia requereixen d'un inici de sessió amb usuari i contrasenya.
		9.4.3. Gestió de contrasenyes d'usuari.	L2	Els usuaris poden canviar la seva contrasenya amb enllaços proporcionats per la companyia, però no obliga a ingressar contrasenyes segures.
		9.4.4. Ús d'eines d'administració de sistemes.	L1	Existeixen polítiques per a software no acceptat a la companyia però no són suficients.
		9.4.5. Control d'accés al codi font dels programes.	L2	El departament de sistemes és l'únic que disposa d'accés al codi font, encara que no està documentat els accessos dels diferents integrants del departament.
10. Xifratge				

Dominis	Objectius de control	Controls	CMM	Observacions
	10.1. Controls criptogràfic.			
		10.1.1. Política d'ús dels controls criptogràfics.	L3	Existeix un procediment de signatura electrònica per a un tipus de documentació entregada per la companyia.
		10.1.2. Gestió de claus.	L0	No existeix cap tipus de gestió de les claus criptogràfiques.
11. Seguretat física i ambiental.				
	11.1. Àrees segures.			
		11.1.1. Perímetre de seguretat física.	L4	Existeix un control d'accessos informatitzat i control físics a l'entrada de l'edifici.
		11.1.2. Controls físics d'entrada.	L4	Existeix un control d'accés a l'entrada de l'edifici i del complex d'oficines.
		11.1.3. Seguretat d'oficines, despatxos i recursos.	L4	Els diferents accessos es realitzen mitjançant clau, menys al CPD on existeix un lector d'empremta connectat al software de control d'accés.
		11.1.4. Protecció contra amenaces externes i ambientals.	L4	La companyia disposa d'un generador elèctric en una part elevada per no tindre problemes de funcionament en cas d'inundació i poder garantir el subministrament elèctric del CPD, també es disposa d'un sistema d'extinció d'incendis.
		11.1.5. El treball en àrees segures.	L4	En el cas de treballs al CDP, és disposa d'un procediment de treball ja que la sala disposa d'un sistema d'extinció d'incendis.
		11.1.6. Àrees d'accés públic, càrrega i descàrrega.	No aplica	
	11.2. Seguretat dels equips.			
		11.2.1. Emplaçament i	L3	Els equips es

Dominis	Objectius de control	Controls	CMM	Observacions
		protecció d'equips.		troben ubicats en llocs adequats a la realització de les seves tasques.
		11.2.2. Instal·lacions de subministre.	L4	Els equips del CPD es tenen unitats SAI i un generador per garantir el subministrament elèctric.
		11.2.3. Seguretat del cablejat.	L4	El cablejat es troba controlat, aïllat i amb tota la instal·lació documentada i certificada.
		11.2.4. Manteniment dels equips.	L4	Els equips es troben en constant manteniment de les seves aplicacions i necessitats. Tenim documentat el procediment d'actualitzacions d'antivirus i software Microsoft.
		11.2.5. Sortida d'actius fora de les dependencies de l'empresa.	L4	Es registren totes les peticions de sortida d'actius mitjançant incidència.
		11.2.6. Seguretat dels equips i actius fora de les instal·lacions.	L0	No existeix cap política de seguretat dels actius que surten temporalment de les instal·lacions.
		11.2.7. Reutilització o retirada segura de dispositius d'emmagatzematge.	L2	Es realitza una verificació per part del departament d'infraestructures de la informació de tots els actius abans de reutilitzar-los o retirar-los. Encara que el procediment no es troba documentat.
		11.2.8. Equip informàtic d'usuari desatès.	L1	Als usuaris se'ls indica que notifiquin per incidència qualsevol missatge de seguretat mostrat per l'ordinador. Però no hi ha cap procediment ni cap tipus de formació que rebi l'usuari.
		11.2.9. Política de lloc de treball aclarit i bloqueig de pantalla.	L1	Encara que no existeix cap tipus de política, s'intenta

Dominis	Objectius de control	Controls	CMM	Observacions
				conscienciar als usuaris de la importància d'aquest fet.
12. Seguretat en la operativa.				
	12.1. Responsabilitats i procediments d'operació.			
		12.1.1. Documentació de procediments d'operació.	L0	El procediments no es troben documentats.
		12.1.2. Gestió de canvis.	L3	Es troben documentats els canvis en seguretat física i negoci. Faltaria documentar els canvis en la seguretat dels sistemes d'informació.
		12.1.3. Gestió de capacitats.	L3	Es realitza una previsió anual per part del departament d'infraestructura de la informació.
		12.1.4. Separació d'entorns de desenvolupament, prova i producció.	L2	Els entorns de desenvolupament es troben en xarxes aïllades de la de producció de la companyia.
	12.2. Protecció contra codi maliciós.			
		12.2.1. Controls contra codi maliciós	L4	Existeix un software antivirus que s'actualitza des d'una ubicació interna a tots els equips de la xarxa i s'informa a tots els usuaris de noves amenaces mitjançant noticies a l'Intranet corporativa.
	12.3. Còpies de seguretat.			
		12.3.1. Còpies de seguretat de la informació.	L4	Existeixen polítiques de copia de seguretat per a tots els sistemes centrals, encara que no hi ha proves de recuperació periòdiques.
	12.4. Registre d'activitat i supervisió.			
		12.4.1. Registre i gestió	L3	Queden enregistrats el

Dominis	Objectius de control	Controls	CMM	Observacions
		d'esdeveniments d'activitat.		inicis de sessió dels usuaris en els logs dels servidors.
		12.4.2. Protecció dels registres d'informació.	L1	No es realitza cap tipus de backup dels logs d'accés d'usuaris. Encara que no són accessibles públicament.
		12.4.3. Registres d'activitat de l'administrador i operador del sistema.	L0	No queden registrades les operacions dels administradors.
		12.4.4. Sincronització de rellotges.	L5	Tota la xarxa sincronitza els seus rellotges a nivell de domini, existint un servidor d'hora intern encarregat de la sincronització.
	12.5. Control del software d'explotació			
		12.5.1. Instal·lació del software a sistemes de producció.	L4	Totes les actualitzacions dels sistemes operatius venen controlades per l'administrador mitjançant polítiques del domini.
	12.6. Gestió de la vulnerabilitat tècnica.			
		12.6.1. Gestió de les vulnerabilitats tècniques.	L3	Es controla per part del departament d'infraestructura de la informació les noves vulnerabilitats existents.
		12.6.2. Restriccions a la instal·lació de software.	L0	No existeix cap impediment a instal·lar software per part dels usuaris.
	12.7. Consideracions de les auditories dels sistemes d'informació.			
		12.7.1. Controls d'auditoria dels sistemes d'informació.	L3	Existeixen auditories externes periòdiques.
13. Seguretat a les telecomunicacions.				
	13.1. Gestió de la seguretat a les xarxes.			
		13.1.1. Controls de xarxa.	L2	La companyia disposa d'utilitats per garantir el correcte funcionament de la

Dominis	Objectius de control	Controls	CMM	Observacions
				xarxa. El departament d'infraestructura de la informació s'encarrega d'administrar la electrònica de xarxa i les aplicacions.
		13.1.2. Mecanismes de seguretat associats a serveis de xarxa.	No aplica	El departament d'infraestructura de la informació, encarregat de l'administració de la xarxa, forma part de la companyia, per tant, no disposa d'SLA emesos a la mateixa.
		13.1.3. Segregació de xarxes.	L5	Tota la xarxa es troba segregada en funció del tipus d'equip que es connecta. La documentació es troba a disposició del departament d'infraestructura de la informació.
	13.2. Intercanvi d'informació amb parts externes.			
		13.2.1. Polítiques i procediments d'intercanvi d'informació.	L4	Existeix un procediment de recuperació de sistema en cas de caiguda per poder continuar amb el servei d'intercanvi. Aquest servei es troba gestionat per un tercers, però allotjat a les nostres oficines (no centrals).
		13.2.2. Acords d'intercanvi.	L4	Existeixen transferències d'informació amb tercers per part del departament de RRHH fent servir aplicacions especifiques aportades pel proveïdor.
		13.2.3. Missatgeria electrònica.	L4	Existeixen mecanismes de filtratge de correu electrònic (filtre AntiSpam) administrats pel departament d'infraestructura de la informació, a l'hora d'una rèplica

Dominis	Objectius de control	Controls	CMM	Observacions
				de servei fora de les instal·lacions centrals.
		13.2.4. Acords de confidencialitat i secret.	L3	El departament de RRHH juntament amb el jurídic aporta els documents a signar per els treballadors susceptibles a treballar amb documentació sensible.
14. Adquisició, desenvolupament i manteniment dels sistemes d'informació.				
	14.1. Requisits de seguretat dels sistemes d'informació.			
		14.1.1. Anàlisi i especificació dels requisits de seguretat.	L2	Es poden aplicar els requisits de seguretat als sistemes de la companyia, encara que aquests no es troben documentats.
		14.1.2. Seguretat de les comunicacions en serveis accessibles per xarxes públiques.	L3	Tota informació accessible des de les xarxes públiques passa per un firewall i requereixen de validació mitjançant usuari i contrasenya.
		14.1.3. Protecció de les transaccions per xarxes telemàtiques.	L4	Tota informació accessible des de les xarxes públiques passa per un firewall i requereixen de validació mitjançant usuari i contrasenya. Es disposa de logs per comprovar les connexions.
	14.2. Seguretat als processos de desenvolupament i suport.			
		14.2.1. Política de desenvolupament segur de software.	L3	El departament de sistemes disposa de polítiques per al desenvolupament de software.
		14.2.2. Procediments de control de canvis als sistemes.	L2	Es valora la viabilitat del canvi per part dels responsables del departament de

Dominis	Objectius de control	Controls	CMM	Observacions
				tecnologies de la informació.
		14.2.3. Revisió tècnica de les aplicacions després d'efectuar canvis al sistema operatiu.	L2	El departament d'infraestructura de la informació s'encarrega de controlar la compatibilitat de les aplicacions amb els nous sistemes operatius.
		14.2.4. Restriccions als canvis en els paquets de software.	L2	Tots els canvis realitzats sobre paquets d'instal·lació de software de tercers es generaran pel departament d'infraestructura de la informació de forma controlada.
		14.2.5. Ús de principis d'enginyeria en protecció de sistemes.	L2	El departament d'infraestructura de la informació genera i manté la informació necessària dels sistemes de la companyia.
		14.2.6. Seguretat en entorns de desenvolupament.	L1	Els entorns de desenvolupament no tenen totes les mesures de seguretat desitjables.
		14.2.7. Externalització del desenvolupament de software.	L5	El departament d'infraestructura de la informació es troba en constant comunicació amb els proveïdors de desenvolupament o adaptació de software.
		14.2.8. Proves de funcionalitat durant el desenvolupament dels sistemes.	L4	Es realitzen diferents proves de funcionalitat per membres del departament de tecnologies de la informació.
		14.2.9. Proves d'acceptació.	L3	Es realitzen enquestes als usuaris per valorar la viabilitat d'implantació de noves versions.
	14.3. Dades de prova.			
		14.3.1. Protecció de les dades utilitzades en proves.	L5	Les dades utilitzades per a les proves no són dades de producció, si no BBDD específiques per aquests processos.

Dominis	Objectius de control	Controls	CMM	Observacions
15. Relacions amb subministradors.				
	15.1. Seguretat de la informació a les relacions amb subministradors.			
		15.1.1. Política de seguretat de la informació per a subministradors.	L4	La companyia disposa de polítiques i procediments per a controlar l'accés de tercers als seus sistemes.
		15.1.2. Tractament del risc dintre dels acords de subministradors.	L3	La companyia disposa de contractes amb cadascun dels subministradors.
		15.1.3. Cadena de subministrament en tecnologies de la informació i comunicacions.	L2	La companyia no disposa de tots els acords amb els proveïdors existents a la cadena de subministrament dels serveis.
	15.2. Gestió de la prestació del servei per subministradors.			
		15.2.1. Supervisió i revisió del serveis prestats per tercers.	L1	La companyia realitza revisions sobre els serveis de tercers en cas de fallida.
		15.2.2. Gestió de canvis als serveis prestats per tercers.	L3	El departament afectat pels canvis del proveïdor, valora la continuïtat del servei basant-se en la política de la companyia.
16. Gestió d'incidents a la seguretat de la informació.				
	16.1. Gestió d'incidents de seguretat de la informació i millores.			
		16.1.1. Responsabilitats i procediments.	L2	La companyia té nombrats als responsables de cada tipus d'incident encara que no està documentat.
		16.1.2. Notificació dels esdeveniments de seguretat de la informació.	L4	La companyia disposa d'una utilitat de ticketing per a gestionar tots els incidents.
		16.1.3. Notificació de punts dèbils de la seguretat.	L4	Es fa servir la mateixa utilitat que en el punt anterior.
		16.1.4. Valoració	L2	El departament

Dominis	Objectius de control	Controls	CMM	Observacions
		d'esdeveniments de seguretat de la informació i presa de decisions.		d'infraestructures de la informació revisa els incidents més greus.
		16.1.5. Resposta als incidents de seguretat.	L2	La companyia no disposa de procediments documentats, encara que la utilitat d'incidències assigna un temps de resposta en funció de la gravetat del incident.
		16.1.6. Aprenentatge dels incidents de seguretat de la informació.	L2	La companyia no disposa de cap base de coneixement on enregistrar solucions a incidents ocorreguts.
		16.1.7. Recopilació d'evidències.	L1	Només es recopilen dades en cas de problema de seguretat.
17. Aspectes de seguretat de la informació a la gestió de la continuïtat del negoci.				
	17.1. Continuïtat de la seguretat de la informació.			
		17.1.1. Planificació de la continuïtat de la seguretat de la informació.	L4	Existeix un protocol de recuperació dels sistemes crítics.
		17.1.2. Implantació de la continuïtat de la seguretat de la informació.	L1	No està documentat cap procediment que garanteixi el manteniment del nivell de seguretat necessari.
		17.1.3. Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	L3	Es revisen regularment els protocols del control 17.1.1.
	17.2. Redundàncies.			
		17.2.1. Disponibilitat d'instal·lacions per al processament de la informació.	L5	Existeixen sistemes replicats a una seu remota per a solvatar possibles problemes de seguretat al CPD central.
18. Compliment.				
	18.1. Compliment dels requisits legals i contractuals.			

Dominis	Objectius de control	Controls	CMM	Observacions
		18.1.1. Identificació de la legislació aplicable.	L3	Es disposa de documents on es registra la documentació legal que aplica a la companyia.
		18.1.2. Drets de propietat intel·lectual (DPI).	L4	La companyia disposa d'una auditoria de software recent.
		18.1.3. Protecció dels registres de l'organització.	L4	Existeix un procediment de copia d'informació.
		18.1.4. Protecció de dades i privacitat de la informació personal.	L3	Les dades personals dels treballadors no són accessibles per la resta d'usuaris, només per usuaris amb permisos d'accés especials.
		18.1.5. Regulació dels controls criptogràfics.	L3	La companyia disposa d'usuaris amb signatura electrònica per a determinats processos.
	18.2. Revisions de la seguretat de la informació.			
		18.2.1. Revisió independent de la seguretat de la informació.	L4	La companyia està sotmesa a auditories independents de forma periòdica.
		18.2.2. Compliment de les polítiques i normes de seguretat.	L2	No hi ha documentació al respecte.
		18.2.3. Comprovació del compliment.	L2	Encara que es van revisant els diferents sistemes, no hi ha documentació al respecte.

Taula 15: Controls ISO/IEC 27002 valorats mitjançant CMM.

9.2. Annex 2: Política de seguretat.

Títol: **Política de seguretat**	Elaborat per: Jsanchezce Data: 20/04/2016	Versió: 1	Revisat per: Data:

Índex:

Objectiu:

Es definirà una política de seguretat de la informació per a l'SGSI on es definiran els nivells de seguretat, confidencialitat, integritat, disponibilitat i continuïtat del servei de la companyia. La direcció notificarà a tota la plantilla la creació de la política i de les diferents guies, normes i estàndards de segon nivell que es desenvolupin per a la seva realització.

Abast:

Les polítiques de seguretat de la companyia afectaran a tots els empleats, proveïdors i externs de la companyia.

Llistat de polítiques:

Es defineixen les següents polítiques de seguretat:

- Teletreball i dispositius mòbils:
  - La sol·licitud d'accés a la companyia per a la realització de tasques de teletreball es realitzarà mitjançant incidència al departament d'infraestructures de la informació.
  - L'accés al correu electrònic de la companyia dels usuaris amb smartphone d'empresa, serà únicament des d'aquest terminal.
  - El tipus de contracte mòbil de cada usuari serà el necessari per a la realització de les seves tasques i serà el departament d'infraestructures de la informació el responsable d'assignar-li.

- La companyia disposa d'una base de dades pròpia amb tota la informació dels mòbils (usuari, IMEI, model, tipus de contracte...).

- Política de connexions remotes: els usuaris que necessitin de connexió remota mitjançant VPN, hauran d'obrir una incidència amb el departament d'infraestructures de la informació, des d'on se li instal·larà el software per a la connexió, es donarà d'alta l'usuari i la contrasenya que haurà de canviar al primer inici de sessió i s'assignarà una caducitat del compte.
- Política de seguretat de la informació de recursos humans: el departament de recursos humans de la companyia s'encarregarà de comprovar la veracitat de la informació dels empleats (certificats acadèmics i professionals...). El departament de recursos humans s'encarrega d'enviar una incidència al departament d'infraestructures de la informació per a la sol·licitud de permisos d'accés als recursos de la xarxa. Mitjançant l'aplicació propietària d'altes i baixes, el departament de RRHH informa al departament d'infraestructures de la informació d'aquestes modificacions en els empleats.

  Tota la informació relativa al departament de RRHH es troba sota la aplicació de la LOPD.
- Política d'ús d'actius: els actius genèrics tenen com a propietaris als responsables dels departaments, mentre que cada usuari que disposi d'un actiu assignat serà responsable d'ell. Només es podran fer servir credencials d'inici de sessió establertes pel departament d'infraestructures de la informació. Els usuaris són els responsables del correcte ús de la informació. Tots els actius han de ser retornats per part dels usuaris al departament d'infraestructures de la informació al finalitzar la seva relació laboral amb la companyia.
- Política de manipulació i arxiu de la informació: la classificació de la informació la definirà cada departament i la notificarà al departament d'infraestructures de la informació. La informació es classificarà d'acord als requisits legals i respectant la LOPD.

- Política de manipulació de dispositius: tots els dispositius s'emmagatzemen de forma segura i de manera externa, en el cas de les còpies de seguretat de la companyia. Es destruirà tota la informació quan un dispositiu es retiri.
- Política de control d'accés lògic: tots els accessos als servidors d'informació de la companyia es sol·licitaran al departament d'infraestructures de la informació per el director del departament o del projecte mitjançant incidència. Aquests permisos d'accés només es poden administrar pel departament d'infraestructures de la informació. La companyia disposa de tres nivells d'accés que són el d'Administrador, Col·laborador o Lector. El departament d'infraestructures de la informació revisarà els permisos d'accés als sistemes cada 6 mesos. Quan es notifica la baixa d'un usuari mitjançant l'aplicació pròpia d'altes i baixes, els permisos d'accés seran anul·lats.
- Política de control de contrasenyes: les contrasenyes de la companyia tindran les característiques següents:
    - Longitud mínima de 8 caràcters.
    - Compostes per lletres i números.
    - Tenen una caducitat de 3 mesos.

  Així mateix, les contrasenyes són personals i intransferibles i és responsabilitat de l'usuari el bon ús de les mateixes.
- Política de control d'accessos remots: els accessos remots als sistemes de la companyia es realitzen únicament mitjançant connexió VPN. Encara que la companyia disposa d'aplicacions pròpies a la seva Intranet corporativa amb accés segur mitjançant HTTPS i validació LDAP.
- Política de control d'accés físic: totes les persones que accedeixen a la companyia (treballadors o visitants) han d'identificar-se als accessos de la mateixa. Els edificis disposen de vídeo vigilància.
- Política d'operacions d'anti-malware: tots els ordinadors, tant personals com servidors, disposen d'una aplicació anti-malware

instal·lada, auto actualitzada, administrada pel departament d'infraestructures de la informació mitjançant consola d'administració on es generen i despleguen les diferents polítiques. Els servidors de correu electrònic disposen d'una aplicació anti-spam proporcionada pel mateix proveïdor que el software anti-malware.

- Política d'operacions de seguretat en aplicacions: els permisos de les diferents aplicacions únicament els pot aplicar l'administrador de l'aplicació, aquestes modificacions li arribaran per sol·licitud del director del departament o del projecte. El departament d'infraestructures de la informació realitza còpies de seguretat de totes les aplicacions, aquestes còpies es realitzen diària, setmanal i mensualment, les còpies mensuals s'emmagatzemen fora de la companyia.
- Política d'operacions de monitoratge dels sistemes: el monitoratge dels sistemes el realitza, pel departament d'infraestructures de la informació o una altra persona a la qual se li delegui la funció, cada dia.
- Política de seguretat en les comunicacions per email: tot el correu entrant i sortint de la companyia passa per un filtre anti-spam, el departament d'infraestructures de la informació s'encarrega del monitoratge del correu electrònic. Els usuaris són coneixedors de que l'ús de l correu electrònic és únicament per a temes laborals, sent ells els responsables de la informació enviada. Tot el contingut de les diferents bústies de correu electrònic es troba sota la influència de la LOPD.

9.3. Annex 3: Procediment d'auditories internes.

Títol: **Procediment d'auditories internes**	Elaborat per: Jsanchezce Data: 20/04/2016	Versió: 1	Revisat per: Data:

Índex:

Objectiu:

Per a l'avaluació del sistema SGSI de la companyia serà necessària la realització d'auditories internes amb una periodicitat establerta.

Abast:

Les auditories es planificaran en funció de la importància dels processos i de les diferents àrees afectades, així com del resultat d'auditories anteriors que recuperarem dels registres.

Equip auditor:

S'ha d'establir un equip auditor ben definit amb un auditor en cap i per part de la companyia hi ha d'haver un responsable de seguretat i un representant de la direcció. El responsable de l'auditoria no pot haver intervingut al procés a auditar.

Fases de l'auditoria interna:

El pla d'auditoria de la companyia esta format per les fases següents:

- Preparació de l'auditoria: el responsable de l'auditoria ha de notificar a totes les parts afectades la planificació de l'auditoria que es durà a terme.
- Realització de l'auditoria: durant aquesta fase, es comprova que tots els departaments afectats tenen la documentació actualitzada, els controls verificats i els procediments actualitzats com indica el SGSI de la companyia. L'auditor s'encarrega de

sol·licitar aquesta documentació als responsables dels departaments auditats.

- Conclusions de l'auditoria: un cop realitzada la fase d'auditoria, l'auditor en cap ha de realitzar l'informe d'auditoria que contindrà totes les no conformitats detectades, les recomanacions de millores en el SGSI i les accions preventives i correctives necessàries, fent servir les plantilles de la companyia.
  Les no conformitats detectades seran notificades a les persones afectades per a la seva correcció.
- Seguiment de l'auditoria: aquesta fase serveix per a que l'auditor pugui comprovar la correcta solució de les no conformitats detectades en el procés d'auditoria, aquests nous resultats els ha d'incloure al document final d'auditoria indicant si la no conformitat ha quedat resolta de forma satisfactòria.

Descripció i periodicitat de les auditories:

La planificació de la companyia per a la realització de les auditories internes de la política de seguretat queda establerta de la manera següent:

- Teletreball i dispositius mòbils: es realitzarà una auditoria del contingut de la base de dades amb la informació dels dispositius mòbils de la companyia cada 18 mesos.
- Política de connexions remotes: es comprovaran els usuaris actius per a la connexió VPN amb la companyia cada 6 mesos.
- Política de seguretat de la informació de recursos humans: es realitza una comprovació dels usuaris donats d'alta al sistema (Directori Actiu) cada 6 mesos, així mateix, el departament de RRHH ha de comprovar que la documentació compleixi amb la LOPD cada any.
- Política d'ús d'actius: es realitza un inventari dels actius de la companyia cada any per poder comprovar la correcta assignació del mateixos a la base de dades de al companyia.

- Política de manipulació i arxiu de la informació: es comprovarà el correcte compliment de la LOPD cada any.
- Política de manipulació de dispositius: es comprovarà el correcte emmagatzematge dels dispositius cada any.
- Política de control d'accés lògic: es realitzarà la verificació de permisos d'accés a la informació del usuaris de la companyia cada 6 mesos.
- Política de control de contrasenyes: la política de contrasenyes s'ha de comprovar si canvia la norma o com a mínim un cop cada tres anys.
- Política de control d'accessos remots: queda verificada amb l'auditoria de la política de connexions remotes.
- Política de control d'accés físic: s'han de verificar els contractes de manteniment amb l'empresa de seguretat cada any i el correcte funcionament del mateix cada 6 mesos.
- Política d'operacions d'anti-malware: es verifiquen els logs de l'aplicació de seguretat anti-mailware/anti-virus cada tres mesos per comprovar la correcta administració duta a terme pel departament d'infraestructures de la informació.
- Política d'operacions de seguretat en aplicacions: es duran a terme auditories internes cada 6 mesos per comprovar la correcta assignació d'usuaris a les diferents aplicacions de la companyia. Les còpies de seguretat s'auditaran cada tres mesos per comprovar la seva capacitat de recuperació.
- Política d'operacions de monitoratge dels sistemes: es verificaran els logs dels sistemes cada any.
- Política de seguretat en les comunicacions per email: es realitzarà un control de la política cada 6 mesos per verificar el correcte funcionament de la seguretat en el correu electrònic.

9.4. Annex 4: Gestió d'indicadors.

Títol: **Gestió d'indicadors**	Elaborat per: Jsanchezce Data: 20/04/2016	Versió: 1	Revisat per: Data:

Índex:

Objectiu:

La companyia necessita poder mesurar l'eficiència dels controls implantats.

Abast:

La gestió d'indicadors s'aplicarà als controls de la ISO/IEC 27002 més crítics del SGSI de la companyia.

Llistat d'indicadors:

Per a poder realitzar aquesta medició, a part de tota la documentació que disposa la companyia generada per l'SGSI, utilitzarem una sèrie d'indicadors per a alguns dels controls:

Control	Indicador	Descripció	Fórmula	Valor objectiu	Valor llindar
6.2.1. Política d'ús de dispositius per a la mobilitat.	Dispositius mòbils de la companyia.	Es mesuren la quantitat de dispositius mòbils registrats.	(Usuaris amb mòbil/Mòbils totals)x100	100%	90%
6.2.2. Teletreball.	Usuaris VPN	Es mesuren els accessos mitjançant VPN per veure quants fallits hi han.	(Accessos fallits / Accessos totals)x100	0%	5%
8.1.1. Inventari d'actius.	Inventari d'actius de la companyia	Es comprova la quantitat d'actius que disposa la companyia	Número total d'actius	±10	±30
8.1.2. Propietat dels actius.	Assignació dels actius de la companyia.	Es verifica que els actius de la companyia estiguin assignats.	(Total actius assignats / Total actius)x100	100%	90%
8.1.3. Ús acceptable dels actius.	Identificació dels actius de la companyia.	Es comprova quins actius no es troben identificats.	Quantitat d'actius sense identificar.	0%	5%
8.1.4. Devolució d'actius.	Devolució dels	Es mesura que els actius tornin a	(Total actius	100%	95%

Control	Indicador	Descripció	Fórmula	Valor objectiu	Valor llindar
	actius a la companyia	la companyia al desaparèixer la relació laboral.	tornats / Total baixes)x100		
8.2.2. Etiquetatge i manipulació de la informació.	Etiquetatge de la informació.	Es mesura la quantitat de documentació que es troba classificada	Total d'informació etiquetada	100%	95%
8.3.1. Gestió de suports extraïbles.	Emmagatzematge de les còpies de seguretat	Es comprova que totes les còpies de seguretat mensuals de la companyia s'emmagatzemen fora del edifici.	Total de còpies emmagatzemada fora de l'edifici.	100%	95%
8.3.2. Eliminació de suports.	Eliminació dels suports retirats.	Total de suports eliminats correctament per a retirar-los de la companyia.	(Total de suports eliminats/Total de suports retirats)x100	100%	95%
9.1.2. Control d'accés a les xarxes i serveis associats.	Accés dels usuaris a les diferents aplicacions corporatives.	Es verifica la correcta assignació de permisos a les aplicacions pròpies de la companyia	% d'incidències per problemes d'accés a les aplicacions.	0%	10%
9.2.1. Gestió d'altes/baixes al registre d'usuaris.	Altes i baixes d'usuaris al sistema.	Verificació del correcte funcionament de l'aplicació d'altes i baixes de la companyia.	Total de altes o baixes no notificades.	0%	5%
9.2.2. Gestió dels drets d'accés assignats a usuaris.	Drets d'accés dels usuaris als recursos de la companyia.	Es verifica que els usuaris només tenen accés al recursos necessaris.	(Accessos necessaris / Accessos assignats)x100	100%	90%
9.2.5. Revisió dels drets d'accés dels usuaris.	Revisió semestral dels permisos dels usuaris.	Total de revisions realitzades en l'últim any	Total de revisions realitzades en l'últim any.	2	2
9.2.6. Retirada o adaptació dels drets d'accés.	Retirada dels drets d'usuaris donats de baixa.	Comprovació de la eliminació dels drets d'usuaris donats de baixa.	(Total de baixes / Total usuaris amb drets retirats per baixa)x100	100%	85%
11.1.1. Perímetre de seguretat física.	Software de control d'accés.	Revisió dels registres del software de control d'accés.	(Accessos erronis / Accessos totals)x100	0%	5%
11.1.3. Seguretat d'oficines, despatxos i recursos.	Software de control d'accés	Revisió dels diferents accessos permesos al CPD	Total de revisions	2	2

Control	Indicador	Descripció	Fórmula	Valor objectiu	Valor llindar
		cada 6 mesos.	realitzades a l'any.		
11.1.4. Protecció contra amenaces externes i ambientals.	Sistema d'alimentació ininterromput.	Estat del generador elèctric de l'edifici, es realitzen proves de funcionament.	(Total proves correcte / Total proves realitzades)x100	100%	95%
12.2.1. Controls contra codi maliciós	Software anti-virus de la companyia.	Revisió del correcte funcionament del programa anti-virus amb revisions dels equips.	(Total equips protegits / Total equips)x100	100%	95%
12.3.1. Còpies de seguretat de la informació.	Còpies de seguretat del CPD central.	Mesura l'eficàcia del control de backups.	(Còpies fallides / Còpies totals)x100	0%	5%
13.2.3. Missatgeria electrònica.	Filtre AntiSpam	Verificació de l'eficàcia del filtre AntiSpam	(Spam aturat / Spam total)x100	100%	95%
13.2.4. Acords de confidencialitat i secret.	Documentació dels acords de confidencialitat	Revisió dels contractes de confidencialitat amb proveïdors.	(Total de contractes / Total de proveïdors)x100	100%	95%
12.4.1. Registre i gestió d'esdeveniments d'activitat.	Registre dels logs dels servidors.	Verificació d'errors als servidors.	(Total d'errors / Total de registres)x100	0%	10%
7.1.2. Termes i condicions de contractació.	Document amb les condicions de la companyia amb el treballador.	Revisió del document amb la normativa de la companyia que s'entrega als treballadors.	Número de revisions anuals.	1	1
9.4.3. Gestió de contrasenyes d'usuari.	Política de contrasenyes.	Revisió de la política de contrasenyes de la companyia.	Número de revisions anuals.	1	1

Taula 16: Indicadors.

9.5. Annex 5: Gestió de rols i resposabilitats.

Títol: **Gestió de rols i responsabilitats**	Elaborat per: Jsanchezce Data: 20/04/2016	Versió: 1	Revisat per: Data:

Índex:

Objectiu:

En aquest punt es definiran els diferents rols i funcions amb els seus responsables i responsabilitats del SGSI dins de la companyia.

Abast:

La gestió de rols i responsabilitats s'aplicarà a tot el personal de la companyia.

Llistat de rols i funcions amb responsables:

A la següent taula podem veure els responsables per a cada rol o funció:

Rols – Funcions al SGSI	Responsables
Organització general de la companyia.	Direcció de la companyia.
Classificació i/o avaluació dels actius del SGSI.	- Hardware, Software i Telecomunicacions: Administradors de sistemes i Responsable del SGSI. - Instal·lacions i equipaments: Administradors de sistemes i Responsable del SGSI. - Dades: els propietaris de les dades i els caps de projectes.
Protecció de les dades	Propietaris de les dades i els administradors de sistemes.
Control d'accés a les aplicacions, sistemes i arxius.	- Accés físic: Responsable del SGSI i la direcció. - Accés lògic: la direcció i els administradors de sistemes.
Personal de seguretat	La direcció, caps de projecte, RRHH i el responsable del SGSI.
Ús dels actius del SGSI.	Tots els usuaris.
Serveis i operacions de TI	Administradors de sistemes.
Seguretat de la xarxa.	Administradors de sistemes.
Manteniment del Software.	Administradors de sistemes.
Gestió de la continuïtat del negoci.	Administradors de sistemes, responsable del SGSI, direcció i caps de projectes.
Externalització de TI	Administradors de sistemes i responsable del SGSI.
Seguretat física.	Administradors de sistemes, responsable del SGSI i direcció.
Seguretat en les aplicacions.	Administradors de sistemes i responsable del SGSI.

Rols – Funcions al SGSI	Responsables
Gestió d'incidències.	Administradors de sistemes i responsable del SGSI. Amb la participació dels usuaris involucrats.
Control de proveïdors i compres.	Direcció i caps de projectes.
Monitoratge dels sistemes.	Administradors de sistemes i responsable del SGSI.
Anàlisi de riscos.	Responsable del SGSI.
Compliment global.	Responsable del SGSI i direcció.

Taula 17: Responsables per rols.

Responsabilitats per rol:

Tot seguit podem veure les diferents responsabilitats que té cada Rol/Responsable:

- Responsable del SGSI:
  - Forma part del comitè de seguretat.
  - Implementació i disseny del SGSI.
  - Verifica la conformitat del SGSI segons la norma.
  - Informa a la direcció del canvis de la norma, legislació... en relació al SGSI.
  - Informa a la direcció de la avaluació dels riscos de seguretat del SGSI.
  - Dissenya, documenta i supervisa la implementació de les polítiques de seguretat.
  - Coordina el tractament dels incidents de seguretat.
  - Planifica, coordina i avalua la formació del personal segons l'SGSI.
  - Millora de forma continua el SGSI.
  - Planifica, prepara i implementa les auditories internes i reporta els resultats a la direcció.
  - Prepara les revisions del SGSI amb la direcció.
- Direcció de la companyia:
  - Tindrà representació dins del comitè de seguretat.
  - El directiu que forma part del comitè de seguretat tindrà les responsabilitats següents:
    - Revisió periòdiques del SGSI.
    - Aprovació de les modificacions del SGSI.
    - Aprovació de les millores del SGSI.
  - Són usuaris amb privilegis d'accés a la informació, especials.
- Administradors de sistemes:
  - Tindrà representació dins del comitè de seguretat.
  - L'administrador que forma part del comitè de seguretat tindrà les responsabilitats següents:
    - Revisió dels controls i dels indicadors del SGSI.
  - Són usuaris amb privilegis d'accés a la informació, especials.
  - Vetllaran per la seguretat de les dades, comunicacions i sistemes.

    - Administració de les còpies de seguretat de la companyia.
    - Revisió dels accessos del usuaris.
    - Coordinació amb les empreses de serveis de TI externes.
    - Gestió de les incidències.
- Caps de projecte:
    - Tindrà representació dins del comitè de seguretat.
    - El cap de projecte que forma part del comitè de seguretat tindrà les responsabilitats següents:
        - Supervisió dels accessos a les dades dels usuaris.
    - Són usuaris amb privilegis d'accés a la informació, especials.
    - Sol·licitaran els accessos a la informació i la denegació dels mateixos quan sigui necessari.
- RRHH:
    - Tindrà representació dins del comitè de seguretat.
    - El representant de RRHH que forma part del comitè de seguretat, tindrà les responsabilitats següents:
        - Proporcionarà els mecanismes necessaris de formació.
    - Són usuaris amb privilegis d'accés a la informació, especials.
- Tots els usuaris:
    - Vetllaran per la confidencialitat de les dades de la companyia.
    - Comunicació de les incidències de seguretat detectades o sospitades.
    - Han de conèixer la normativa de la companyia.
    - Han de fer un bon ús de les seves credencials segons la política de seguretat del SGSI.
    - Fer un bon ús dels actius de la companyia que tinguin assignats o siguin d'ús comú.
    - Fer entrega dels actius de la companyia quan deixin de prestar servei en la mateixa.

9.6. Annex 6: Plantilla d'inventari d'actius.

Tot seguit tenim dues plantilles per a la realització de l'inventari d'actius hardware i terminals mòbils:

- Plantilla d'inventari Hardware:

ID:	Nom equip:	Empresa:
Tipus:	**Marca:**	**S/N:**
Model:	**Data alta:**	**Data baixa:**
Disc dur (TB):	**RAM (GB):**	**SO:**
Descripció:		
Assignació		
Tipus:	**Departament:**	
Usuari:	**Data alta:**	**Data baixa:**
Ubicació:		
Observacions:		

- Plantilla d'inventari dispositius mòbils:

ID:	Empresa:	
Tipus:	**Marca:**	**Model:**
IMEI:	**Data alta:**	**Data baixa:**
ICC:	**Núm. mòbil:**	**PUK:**
Descripció:		
Assignació		
Tipus:	**Departament:**	
Usuari:	**Data alta:**	**Data baixa:**
Ubicació:		
Observacions:		

9.7. Annex 7: Declaració d'aplicabilitat.

Títol: **Declaració d'aplicabilitat**	Elaborat per: Jsanchezce Data: 20/04/2016	Versió: 1	Revisat per: Data:

Índex:

Objectiu:

Especificar l'aplicabilitat dels controls de la norma ISO/IEC 27002:2013 sobre el SGSI de la companyia.

Abast:

La declaració d'aplicabilitat es realitza sobre tots els controls de la norma ISO/IEC 27002:2013.

Llistat d'aplicabilitat per controls:

A la següent taula podem veure la declaració d'aplicabilitat dels diferents controls de la companyia, on s'indica si s'estan aplicant i la documentació associada a ells:

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
5. Polítiques de Seguretat				
	5.1. Directrius de la Direcció en seguretat de la informació			
		5.1.1. Conjunt de polítiques per a la seguretat de la informació.	SI	SGSI_INGENSA Pol_SGSI_Seg-Inf
		5.1.2. Revisió de les polítiques per a la seguretat de la informació.	SI	SGSI_INGENSA Pol_SGSI_Seg-Inf
6. Aspectes Organitzatius de la seguretat de la informació				
	6.1. Organització Interna.			
		6.1.1. Assignació de responsabilitats per a la seguretat de la	SI	SGSI_INGENSA Pol_SGSI_Seg-Inf SGSI_Resp_Seg-Inf

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
		informació.		
		6.1.2. Segregació de taques.	SI	SGSI_INGENSA SGSI_Resp-Seg-Inf
		6.1.3. Contacte amb les autoritats.	SI	SGSI_INGENSA Pol_SGSI_Compliment SGSI_Gest-Inc
		6.1.4. Contacte amb els grups d'interès especial.	SI	SGSI_INGENSA Pol_SGSI_Compliment
		6.1.5. Seguretat de la informació a la gestió de projectes.	SI	SGSI_Avaluacio-Risc Pol_SGSI_Canvis
	6.2. Dispositius per a la mobilitat i el teletreball.			
		6.2.1. Política d'ús de dispositius per a la mobilitat.	SI	SGSI_Actius-Us Pol_SGSI_Mobils Pol_SGSI_Manip-Med
		6.2.2. Teletreball.	SI	SGSI_Actius-Us Pol_SGSI_Mobils Pol_SGSI_Manip-Med
7. Seguretat lligada als recursos humans.				
	7.1. Abans de la contractació.			
		7.1.1. Investigació d'antecedents.	SI	SGSI_Requis-Contrac Pol_SGSI_RRHH Pol_RRHH_Personal
		7.1.2. Termes i condicions de contractació.	SI	SGSI_Requis-Contrac Pol_SGSI_RRHH Pol_RRHH_Personal Pol_SGSI_Seg-Inf
	7.2. Durant la contractació.			
		7.2.1. Responsabilitats de gestió.	SI	Pol_SGSI_Seg-Inf
		7.2.2. Conscienciació, educació i capacitació en seguretat de la informació.	SI	Pol_SGSI_RRHH Pol_RRHH_Personal
		7.2.3. Procés disciplinari.	SI	Pol_SGSI_RRHH Pol_RRHH_Personal
	7.3. Cessament o canvi de lloc de treball.			
		7.3.1. Cessament o canvi de lloc de treball.	SI	Pol_SGSI_RRHH SGSI_Actius-Us Pol_SGSI_Contr-Acc
8. Gestió d'actius.				
	8.1. Responsabilitat sobre els actius.			
		8.1.1. Inventari d'actius.	SI	SGSI_Invent-Actius SGSI_Avaluacio-Risc
		8.1.2. Propietat dels actius.	SI	SGSI_Invent-Actius SGSI_Avaluacio-Risc
		8.1.3. Ús acceptable dels actius.	SI	SGSI_Actius-Us
		8.1.4. Devolució d'actius.	SI	SGSI_Actius-Us Pol_SGSI_Contr-Acc

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
				Pol_SGSI_RRHH
	8.2. Classificació de la informació.			
		8.2.1. Directrius de classificació.	SI	Pol_SGSI_Classif-Inf SGSI_Invent-Actius SGSI_Avaluacio-Risc
		8.2.2. Etiquetatge i manipulació de la informació.	SI	Pol_SGSI_Classif-Inf
		8.2.3. Manipulació d'actius.	SI	SGSI_Actius-Us Pol_SGSI_Classif-Inf Pol_SGSI_Manip-Med
	8.3. Maneig dels suports d'emmagatzematge			
		8.3.1. Gestió de suports extraïbles.	SI	Pol_SGSI_Mobils Pol_SGSI_Manip-Med
		8.3.2. Eliminació de suports.	SI	Pol_SGSI_Manip-Med Pol_SGSI_Classif-Inf SGSI_Actius-Us
		8.3.3. Suports físics en transit.	SI	Pol_SGSI_Manip-Med Pol_SGSI_Mobils Pol_SGSI_Cripto
9. Control d'accés.				
	9.1. Requisits de negoci per al control d'accessos.			
		9.1.1. Política de control d'accessos.	SI	Pol_SGSI_Contr-Acc Pol_SGSI_Contrasenya Pol_SGSI_Acces-Rem
		9.1.2. Control d'accés a les xarxes i serveis associats.	SI	Pol_SGSI_Contr-Acc Pol_SGSI_Contrasenya Pol_SGSI_Xarxa-Seg
	9.2. Gestió d'accés d'usuari.			
		9.2.1. Gestió d'altes/baixes al registre d'usuaris.	SI	Pol_SGSI_Contr-Acc Pol_SGSI_Contrasenya
		9.2.2. Gestió dels drets d'accés assignats a usuaris.	SI	Pol_SGSI_Contr-Acc
		9.2.3. Gestió dels drets d'accés amb privilegis especials.	SI	Pol_SGSI_Contr-Acc
		9.2.4. Gestió d'informació confidencial d'autenticació d'usuaris.	SI	Pol_SGSI_Contrasenya
		9.2.5. Revisió dels drets d'accés dels usuaris.	SI	Pol_SGSI_Contr-Acc Pol_SGSI_Contrasenya
		9.2.6. Retirada o adaptació dels drets d'accés.	SI	Pol_SGSI_Contr-Acc Pol_SGSI_Contrasenya Pol_SGSI_RRHH
	9.3. Responsabilitats de l'usuari.			
		9.3.1. Ús d'informació confidencial per a l'autenticació.	SI	Pol_SGSI_Contrasenya Pol_SGSI_RRHH SGSI_Actius-Us

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
	9.4. Control d'accés a sistemes i aplicacions.			
		9.4.1. Restricció de l'accés a la informació	SI	Pol_SGSI_Contr-Acc Pol_SGSI_Contrasenya
		9.4.2. Procediments segurs d'inici de sessió.	SI	Pol_SGSI_Contr-Acc Pol_SGSI_Contrasenya Pol_SGSI_Xarxa-Seg Pol_SGSI_Acces-Rem
		9.4.3. Gestió de contrasenyes d'usuari.	SI	Pol_SGSI_Contrasenya
		9.4.4. Ús d'eines d'administració de sistemes.	SI	Pol_SGSI_Contr-Acc Pol_SGSI_Contrasenya Pol_SGSI_Xarxa-Seg
		9.4.5. Control d'accés al codi font dels programes.	SI	Pol_SGSI_Contr-Acc Pol_SGSI_Contrasenya Pol_SGSI_Xarxa-Seg
10. Xifratge				
	10.1. Controls criptogràfic.			
		10.1.1. Política d'ús dels controls criptogràfics.	SI	Pol_SGSI_Cripto Pol_SGSI_Mobils
		10.1.2. Gestió de claus.	NO	No existeix cap política degut a que les claus criptogràfiques existents són personals.
11. Seguretat física i ambiental.				
	11.1. Àrees segures.			
		11.1.1. Perímetre de seguretat física.	SI	Pol_SGSI_Contr-Acc
		11.1.2. Controls físics d'entrada.	SI	Pol_SGSI_Contr-Acc
		11.1.3. Seguretat d'oficines, despatxos i recursos.	SI	Pol_SGSI_Contr-Acc
		11.1.4. Protecció contra amenaces externes i ambientals.	SI	Pol_SGSI_Contr-Acc
		11.1.5. El treball en àrees segures.	SI	Pol_SGSI_Contr-Acc
		11.1.6. Àrees d'accés públic, càrrega i descàrrega.	NO	La companyia no disposa d'àrees d'aquest tipus.
	11.2. Seguretat dels equips.			
		11.2.1. Emplaçament i protecció d'equips.	SI	SGSI_Invent-Actius Pol_SGSI_Contr-Acc Pol_SGSI_Lloc-Treball SGSI_Actius-Us Pol_SGSI_Proveidors
		11.2.2. Instal·lacions de subministre.	SI	SGSI_Invent-Actius
		11.2.3. Seguretat	SI	Pol_SGSI_Seg_LAN

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
		del cablejat.		
		11.2.4. Manteniment dels equips.	SI	SGSI_Actius-Us Pol_SGSI_Proveidors
		11.2.5. Sortida d'actius fora de les dependencies de l'empresa.	SI	SGSI_Actius-Us
		11.2.6. Seguretat dels equips i actius fora de les instal·lacions.	SI	Pol_SGSI_Mobils
		11.2.7. Reutilització o retirada segura de dispositius d'emmagatzematge.	SI	SGSI_Actius-Us Pol_SGSI_Classif-Inf
		11.2.8. Equip informàtic d'usuari desatès.	SI	SGSI_Actius-Us Pol_SGSI_Lloc-Treball
		11.2.9. Política de lloc de treball aclarit i bloqueig de pantalla.	SI	Pol_SGSI_Lloc-Treball
12. Seguretat en la operativa.				
	12.1. Responsabilitats i procediments d'operació.			
		12.1.1. Documentació de procediments d'operació.	SI	SGSI_INGENSA
		12.1.2. Gestió de canvis.	SI	Pol_SGSI_Canvis
		12.1.3. Gestió de capacitats.	SI	Pol_SGSI_Canvis
		12.1.4. Separació d'entorns de desenvolupament, prova i producció.	SI	Pol_SGSI_Xarxa-Seg
	12.2. Protecció contra codi maliciós.			
		12.2.1. Controls contra codi maliciós	SI	Pol_SGSI_Malware Pol_SGSI_Xarxa-Seg Pol_SGSI_Acces-Rem
	12.3. Còpies de seguretat.			
		12.3.1. Còpies de seguretat de la informació.	SI	Pol_SGSI_Backup
	12.4. Registre d'activitat i supervisió.			
		12.4.1. Registre i gestió d'esdeveniments d'activitat.	SI	Pol_SGSI_Logs Pol_SGSI_Canvis
		12.4.2. Protecció dels registres d'informació.	SI	Pol_SGSI_Logs
		12.4.3. Registres	SI	Pol_SGSI_Logs

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
		d'activitat de l'administrador i operador del sistema.		
		12.4.4. Sincronització de rellotges.	SI	Pol_SGSI_Logs
	12.5. Control del software d'explotació			
		12.5.1. Instal·lació del software a sistemes de producció.	SI	Pol_SGSI_Seg-Aplic SGSI_Actius-Us
	12.6. Gestió de la vulnerabilitat tècnica.			
		12.6.1. Gestió de les vulnerabilitats tècniques.	SI	SGSI_Avaluacio-Risc Pol_SGSI_Canvis Pol_SGSI_Compliment
		12.6.2. Restriccions a la instal·lació de software.	SI	Pol_SGSI_Seg-Aplic SGSI_Actius-Us
	12.7. Consideracions de les auditories dels sistemes d'informació.			
		12.7.1. Controls d'auditoria dels sistemes d'informació.	SI	Pol_SGSI_Canvis Pol_SGSI_Compliment
13. Seguretat a les telecomunicacions.				
	13.1. Gestió de la seguretat a les xarxes.			
		13.1.1. Controls de xarxa.	SI	Pol_SGSI_Xarxa-Seg Pol_SGSI_Seg-Aplic Pol_SGSI_Acces-Rem
		13.1.2. Mecanismes de seguretat associats a serveis de xarxa.	NO	Els proveïdors que ens donen serveis de telecomunicacions no inclouen mecanismes de seguretat als seus SLAs.
		13.1.3. Segregació de xarxes.	SI	Pol_SGSI_Xarxa-Seg
	13.2. Intercanvi d'informació amb parts externes.			
		13.2.1. Polítiques i procediments d'intercanvi d'informació.	SI	Pol_SGSI_Classif-Inf Pol-SGSI_Acces-Rem
		13.2.2. Acords d'intercanvi.	SI	Pol_SGSI_Proveidors
		13.2.3. Missatgeria electrònica.	SI	Pol_SGSI_Email-Seg
		13.2.4. Acords de confidencialitat i secret.	SI	Pol_SGSI_Proveidors
14. Adquisició,				

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
desenvolupament i manteniment dels sistemes d'informació.				
	14.1. Requisits de seguretat dels sistemes d'informació.			
		14.1.1. Anàlisi i especificació dels requisits de seguretat.	SI	SGSI_INGENSA
		14.1.2. Seguretat de les comunicacions en serveis accessibles per xarxes públiques.	SI	Pol_SGSI_Acces-Rem Pol_SGSI_Xarxa-Seg
		14.1.3. Protecció de les transaccions per xarxes telemàtiques.	SI	Pol_SGSI_Acces-Rem Pol_SGSI_Xarxa-Seg Pol_SGSI_Cripto
	14.2. Seguretat als processos de desenvolupament i suport.			
		14.2.1. Política de desenvolupament segur de software.	SI	SGSI_INGENSA
		14.2.2. Procediments de control de canvis als sistemes.	SI	SGSI_INGENSA
		14.2.3. Revisió tècnica de les aplicacions després d'efectuar canvis al sistema operatiu.	SI	SGSI_INGENSA
		14.2.4. Restriccions als canvis en els paquets de software.	SI	SGSI_INGENSA
		14.2.5. Ús de principis d'enginyeria en protecció de sistemes.	SI	SGSI_INGENSA
		14.2.6. Seguretat en entorns de desenvolupament.	SI	SGSI_INGENSA
		14.2.7. Externalització del desenvolupament de software.	SI	SGSI_INGENSA Pol_SGSI_Proveidors
		14.2.8. Proves de funcionalitat durant el desenvolupament dels sistemes.	SI	SGSI_INGENSA
		14.2.9. Proves d'acceptació.	SI	SGSI_INGENSA
	14.3. Dades de prova.			
		14.3.1. Protecció de	SI	SGSI_INGENSA

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
		les dades utilitzades en proves.		
15. Relacions amb subministradors.				
	15.1. Seguretat de la informació a les relacions amb subministradors.			
		15.1.1. Política de seguretat de la informació per a subministradors.	SI	Pol_SGSI_Proveidors
		15.1.2. Tractament del risc dintre dels acords de subministradors.	SI	Pol_SGSI_Proveidors SGSI_Avaluacio-Risc
		15.1.3. Cadena de subministrament en tecnologies de la informació i comunicacions.	SI	Pol_SGSI_Proveidors SGSI_Avaluacio-Risc
	15.2. Gestió de la prestació del servei per subministradors.			
		15.2.1. Supervisió i revisió del serveis prestats per tercers.	SI	Pol_SGSI_Proveidors
		15.2.2. Gestió de canvis als serveis prestats per tercers.	SI	Pol_SGSI_Proveidors Pol_SGSI_Canvis
16. Gestió d'incidents a la seguretat de la informació.				
	16.1. Gestió d'incidents de seguretat de la informació i millores.			
		16.1.1. Responsabilitats i procediments.	SI	Pol_SGSI_Gestio-Inc
		16.1.2. Notificació dels esdeveniments de seguretat de la informació.	SI	Pol_SGSI_Gestio-Inc
		16.1.3. Notificació de punts dèbils de la seguretat.	SI	Pol_SGSI_Gestio-Inc
		16.1.4. Valoració d'esdeveniments de seguretat de la informació i presa de decisions.	SI	Pol_SGSI_Gestio-Inc
		16.1.5. Resposta als incidents de seguretat.	SI	Pol_SGSI_Gestio-Inc SGSI_Cont-Negoci
		16.1.6. Aprenentatge dels	SI	Pol_SGSI_Gestio-Inc

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
		incidents de seguretat de la informació.		
		16.1.7. Recopilació d'evidències.	SI	Pol_SGSI_Gestio-Inc
17. Aspectes de seguretat de la informació a la gestió de la continuïtat del negoci.				
	17.1. Continuïtat de la seguretat de la informació.			
		17.1.1. Planificació de la continuïtat de la seguretat de la informació.	SI	SGSI_Cont-Negoci
		17.1.2. Implantació de la continuïtat de la seguretat de la informació.	SI	SGSI_Cont-Negoci
		17.1.3. Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	SI	SGSI_Cont-Negoci
	17.2. Redundàncies.			
		17.2.1. Disponibilitat d'instal·lacions per al processament de la informació.	SI	SGSI_Invent-Actius Pol_SGSI_Canvis SGSI_Cont-Negoci
18. Compliment.				
	18.1. Compliment dels requisits legals i contractuals.			
		18.1.1. Identificació de la legislació aplicable.	SI	Pol_SGSI_Compliment SGSI_Requis-Legal
		18.1.2. Drets de propietat intel·lectual (DPI).	SI	Pol_SGSI_Compliment SGSI_Requis-Legal
		18.1.3. Protecció dels registres de l'organització.	SI	Pol_SGSI_Classif-Inf SGSI_Invent-Actius Pol_SGSI_Backups
		18.1.4. Protecció de dades i privacitat de la informació personal.	SI	Pol_SGSI_Compliment SGSI_Requis-Legal
		18.1.5. Regulació dels controls criptogràfics.	SI	Pol_SGSI_Compliment SGSI_Requis-Legal Pol_SGSI_Cripto
	18.2. Revisions de la seguretat de la informació.			
		18.2.1. Revisió independent de la seguretat de la informació.	SI	SGSI_INGENSA SGSI_Reg_Audit-Int
		18.2.2. Compliment de les polítiques i normes de	SI	Pol_SGSI_Compliment

Dominis	Objectius de control	Controls	Aplica	Documentació relacionada / Justificació
		seguretat.		
		18.2.3. Comprovació del compliment.	SI	Pol_SGSI_Compliment Pol_SGSI_Canvis

Taula 18: Aplicabilitat dels controls de la companyia.

9.8. Annex 8: Catàleg d'amenaces segons MAGERIT 3.0.

Tot seguit tenim les diferents amenaces que es poden donar a la companyia, agrupades per la seva classificació i amb la dimensió que afecten.

Classificació	Codi MAGERIT de l'amenaça	Descripció	Dimensió				
			A	C	I	D	A
[N] Desastres naturals							
	[N.1]	Foc				X	
	[N.2]	Danys per aigua				X	
	[N.*]	Desastres naturals				X	
[I] D'origen industrial							
	[I.1]	Foc				X	
	[I.2]	Danys per aigua				X	
	[I.*]	Desastres industrials				X	
	[I.5]	Avaria d'origen físic o lògic				X	
	[I.6]	Tall del subministrament elèctric				X	
	[I.7]	Condicions inadequades de temperatura o humitat				X	
	[I.8]	Fallida dels serveis de comunicacions				X	
	[I.9]	Interrupció d'altres serveis i subministraments essencials				X	
[E] Errors i fallides no intencionats							
	[E.1]	Errors dels usuaris		X	X	X	
	[E.2]	Errors de l'administrador		X	X	X	
	[E.7]	Deficiències a l'organització				X	
	[E.9]	Errors de [re-]encaminament		X			
	[E.10]	Errors de seqüència			X		
	[E.15]	Alteració accidental de la informació			X		
	[E.18]	Destrucció de la informació				X	
	[E.19]	Fugues d'informació		X			
	[E.20]	Vulnerabilitats dels programes (software)		X	X	X	
	[E.21]	Errors de manteniment / actualització de programes (software)			X	X	
	[E.23]	Errors de manteniment /actualització d'equips (hardware)				X	
	[E.28]	Indisponibilitat del personal				X	
[A] Atacs intencionats							
	[A.5]	Suplantació de la identitat de l'usuari	X	X	X		
	[A.6]	Abús de privilegis d'accés		X	X	X	
	[A.7]	Ús no previst		X	X	X	
	[A.8]	Difusió de software maliciós		X	X	X	
	[A.9]	[Re-]encaminament de missatges		X			
	[A.10]	Alteració de seqüència			X		
	[A.11]	Accés no autoritzat		X	X		
	[A.12]	Anàlisi de tràfic		X			
	[A.13]	Repudi			X		
	[A.14]	Interceptació de informació (escolta)		X			

Classificació	Codi MAGERIT de l'amenaça	Descripció	Dimensió				
			A	C	I	D	A
	[A.15]	Modificació deliberada de la informació			X		
	[A.18]	Destrucció de informació				X	
	[A.19]	Divulgació de informació		X			
	[A.23]	Manipulació dels equips		X		X	
	[A.24]	Denegació de servei				X	
	[A.25]	Robatori		X		X	
	[A.26]	Atac destructiu				X	
	[A.28]	Indisponibilitat del personal				X	
	[A.29]	Extorsió		X	X	X	
	[A.30]	Enginyeria social (picaresca)		X	X	X	

Taula 19: Catàleg d'amenaces segons MAGERIT 3.0.

9.9. Annex 9: Propostes de projectes.

Tot seguit tenim les diferents propostes de projectes per millorar la seguretat del sistema SGSI de la companyia.

ID: PRO-001	Establiment de la política de seguretat
Descripció: Es crearà un document on es definirà tota la normativa de seguretat referent a la companyia, legislació aplicable, normes obligatòries d'ús per part del personal, normativa per tercers. Aquesta política ha d'estar recolzada per la direcció de la companyia i ha de estar disponible per a tots els treballadors i tercers. La companyia ha d'assegurar-se de la correcta formació del personal. Aquesta política s'ha d'actualitzar amb periodicitat o front a canvis en la estructura de la companyia o de la normativa vigent.	
Objectius: Com a principal objectiu tenim la creació d'una política de seguretat de la informació per a assegurar la disponibilitat, integritat i confidencialitat de la informació de la companyia i de les seves relacions amb tercers. Així com la continuïtat dels serveis. Minimitzar el risc als actius crítics. Garantir contrasenyes segures. Garantir el compliment de la normativa espanyola aplicable a la companyia. Solucionar problemes de seguretat gràcies a la formació al personal.	
Afectació	
Actius: Tots els actius de la companyia.	Dominis ISO/IEC 27002:2013: 5. Polítiques de Seguretat.
Riscos mitigats: Totes les dimensions ACIDA per a tots els actius de la companyia.	
Durada: 4 mesos	**Període de consecució:** Mig

Recursos necessaris	
Personal: - Departament legal. - Departament de RRHH. - Departament d'Infraestructures de la informació. - Direcció. - Responsable de seguretat.	Econòmic: S'estima un cost intern de 3.500€ en funció de les hores dedicades per personal de la companyia.

ID: PRO-002	Document de seguretat per a les noves contractacions

Descripció:

Es crearà un document on es detallaran totes les mesures de seguretat per informar a les noves contractacions i, si fos necessari degut a grans canvis, també es notificarà a la resta de la plantilla. Igual que amb la política de seguretat, aquest document ha d'estar aprovat per la direcció de la companyia.

Objectius:

Com a principal objectiu tenim la redacció del document amb les normes de seguretat que s'han d'aportar a les noves contractacions per a un correcte funcionament de la seguretat de la informació. Establir el procés disciplinari existent a la companyia. Evitar problemes derivats de la falta d'informació d'aquest document.

Afectació

Actius:	Dominis ISO/IEC 27002:2013:
Tot el personal de la companyia.	7. Seguretat lligada als recursos humans.

Riscos mitigats:

Confidencialitat i Integritat per al personal de la companyia.

Durada: 1 mes	**Període de consecució:** Baix

Recursos necessaris

Personal:	Econòmic:
- Departament de RRHH. - Departament d'Infraestructures de la informació. - Direcció. - Responsable de seguretat.	S'estima un cost intern de 1.000€ en funció de les hores dedicades per personal de la companyia.

ID: PRO-003	Document per a establir el protocol de classificació de la informació.

Descripció:

Es crearà un document on es detallarà el protocol a seguir per a la classificació de la informació de la companyia. S'indicaran els diferents nivells de classificació amb la seva seguretat i el procediment a seguir a l'hora de destruir el suport on es trobi la informació. La direcció de la companyia ha de recolzar el document per a una correcta implementació.

Aquest document es revisarà si es realitza algun canvi en la estructura o funcionament de la companyia o per canvis el la legislació vigent.

Objectius:

El principal objectiu és la redacció del document amb el protocol de classificació de la informació de la companyia. S'han de generar els diferents nivells de classificació existents i els processos de seguretat que afectin a cada nivell. S'ha d'aconseguir minimitzar la sortida de informació confidencial cap a tercers no autoritzats. Tota la informació es trobarà correctament classificada i amb els accessos assignats a les persones autoritzades per a cada nivell. Redactar un procediment de destrucció de la informació no útil.

Afectació

Actius:	Dominis ISO/IEC 27002:2013:
Tots els actius de la companyia.	8. Gestió d'actius.

Riscos mitigats:

Totes les dimensions ACIDA per als actius de la companyia que contenen informació, agrupats als àmbits de hardware, aplicacions, dades i serveis.

Durada: 1 mes	**Període de consecució:** Baix

Recursos necessaris

Personal:	Econòmic:
- Departament d'Infraestructures de la informació. - Direcció. - Els directors de departaments. - Responsable de seguretat.	S'estima un cost intern de 1.000€ en funció de les hores dedicades per personal de la companyia.

ID: PRO-004	Implantació d'un MDM

Descripció:

S'implantarà un aplicatiu MDM centralitzat per controlar els diferents dispositius mòbils de la companyia i garantir la seguretat dels mateixos. S'incorporarà el xifratge de la informació, control de consum, eliminació de dades en cas de pèrdua o robatori, configuració dels plans de dades dels Smartphones, configuració dels correus electrònics corporatius, consums, desplegament de polítiques de seguretat en navegació, ús de les dades per evitar còpies no permeses de la informació i la companyia obtindrà un inventari controlat dels diferents dispositius mòbils (telèfons, portàtils i tauletes).

Es formarà a personal del departament d'infraestructures de la informació per l'administració i desplegament de l'eina.

Es requerirà de l'autorització de la direcció per a l'adquisició de l'eina.

Objectius:

Estudi dels diferents softwares MDM disponibles al mercat, instal·lació i formació del que més s'ajusti a les necessitats de la companyia. Control de costos per disminuir la facturació actual. Control de seguretat de les dades mitjançant polítiques per assegurar dades fora de la companyia. Modificació en les configuracions dels terminals. Formació del personal d'infraestructures de la informació per a un correcte manteniment de l'aplicació.

Afectació

Actius:	Dominis ISO/IEC 27002:2013:
- Dispositius mòbils (telèfons, portàtils i tauletes). - Personal del departament d'infraestructures de la informació.	8. Gestió d'actius. 11. Seguretat física i ambiental.

Riscos mitigats:

Confidencialitat, Integritat i Disponibilitat dels dispositius mòbils de la companyia.

Durada: 6 mesos	**Període de consecució:** Alt

Recursos necessaris	
Personal: - Departament d'infraestructures de la informació. - Direcció. - Responsable de seguretat.	Econòmic: Cost de l'aplicació, manteniment i formació de 8.000€.

ID: PRO-005	Procediments per a la documentació de TI

Descripció:

Es realitzaran les diferents plantilles per a documentar els procediments del departament, on apareixerà l'usuari que ha desenvolupat el document, el revisor, la versió, la data de redacció, la introducció, l'abast, l'objectiu i el procediment.

S'hauran de revisar els diferents procediments en cada modificació de les parts involucrades o amb una periodicitat de dos anys.

Objectius:

Unificar els procediments del departament de TI per aconseguir reduir els problemes associats i estandarditzar els processos. Permetre la realització dels diferents procediments per tota la plantilla del departament de TI.

Afectació

Actius:	Dominis ISO/IEC 27002:2013:
Personal del departament de TI.	12. Seguretat a l'operativa.

Riscos mitigats:

Totes les dimensions ACIDA per a tots els actius de la companyia exceptuant els àmbits d'instal·lacions i personal.

Durada: 3 mes	**Període de consecució:** Baix

Recursos necessaris

Personal:	Econòmic:
- Departament de TI. - Responsable de seguretat.	S'estima un cost intern de 2.000€ en funció de les hores dedicades per personal de la companyia.

ID: PRO-006	Política de seguretat per a la instal·lació de software

Descripció:

Es crearà un document on es definiran els diferents tipus de software necessari per als rols existents en la companyia, no es permetrà la instal·lació de software per part del usuaris sense autorització, les aplicacions s'actualitzaran des d'un repositori central en el cas de l'antivirus, sistemes operatius i aplicacions Microsoft. Aquesta política ha d'estar recolzada per la direcció de la companyia.

Aquesta política s'ha d'actualitzar amb periodicitat o front a canvis en les necessitats de treball dels usuaris o noves aplicacions.

Objectius:

Establir els criteris per a la redacció de la política d'instal·lació de software, on s'evitarà la lliure instal·lació d'aplicacions. S'incrementarà la seguretat dels sistemes al estar actualitzats. Es tindrà un millor control de les llicències necessàries i així es reduirà el cost de les mateixes. S'evitarà l'entrada de virus.

Afectació

Actius:	Dominis ISO/IEC 27002:2013:
Tots els ordinadors de la companyia.	11. Seguretat física i ambiental. 12. Seguretat en l'operativa.

Riscos mitigats:

Totes les dimensions ACIDA per als actius de la companyia dels àmbits hardware, aplicacions, dades, xarxa i serveis.

Durada: 1 mes	**Període de consecució:** Alt

Recursos necessaris

Personal:	Econòmic:
- Departament d'infraestructures de la informació. - Direcció. - Responsable de seguretat.	S'estima un cost intern de 1.000€ en funció de les hores dedicades per personal de la companyia.

ID: PRO-007	Seguretat del Hardware i serveis crítics.

Descripció:

Es documentarà un procés per assegurar el hardware més crític de la companyia, com és el cas del Servidor CRM, Servidor de Exchange... Es configurarà una extensió LAN per a disposar del mateix rang IP en dos seus remotes i així poder tindre els serveis duplicats en dos llocs físics diferents per assegurar-los front a desastres. S'estableix un procediment per realitzar una còpia incremental del sistema diàriament en el cas dels sistemes més crítics i setmanalment en els que tinguin una nivell de risc mitjà. S'estableix un procediment de recuperació en cas de desastre per a garantir la continuïtat de negoci de la companyia. El sistema de còpia es revisarà diàriament per part del departament d'infraestructures de la informació.

Es necessitarà l'aprovació de la direcció per a l'aprovació del cost econòmic.

Objectius:

Evitar la pèrdua dels serveis més crítics de la companyia i les dades associades. Reduir el temps de recuperació dels sistemes en cas de desastre. Establir un procediment per a la recuperació del servei.

Afectació

Actius:	Dominis ISO/IEC 27002:2013:
- Hardware crític. - Serveis crítics. - Dades crítiques.	11. Seguretat física i ambiental. 12. Seguretat en l'operativa. 13. Seguretat en les telecomunicacions. 15. Relacions amb els proveïdors. 16. Gestió d'incidents a la seguretat de la informació. 17. Aspectes de seguretat de la informació a la gestió de la continuïtat del negoci.

Riscos mitigats:

Totes les dimensions ACIDA per a tots els actius de la companyia que ofereixen els serveis més crítics (correu electrònic, CRM, dades...), afectant tant al hardware, dades, serveis i aplicació.

Durada: 1 any	**Període de consecució:** Alt
Recursos necessaris	
Personal: - Departament d'infraestructures de la informació. - Direcció. - Proveïdor VPN.	Econòmic: Cost del servidor per emmagatzemar les dades 30.000€. Cost de l'electrònica per configurar l'extensió LAN entre les dues seus 1.500€. Cost personal intern per a la implementació i manteniment del procés 8.000€

ID: PRO-008	Document de control de les còpies de seguretat

Descripció:

S'estableix el procediment d'implantació, configuració i revisió de les còpies de seguretat de les diferents dades de la companyia. S'indicarà la periodicitat per a la realització de les proves de recuperació de dades que es realitzaran per part del departament d'infraestructura de la informació. Es definirà tant l'aplicació de backup a utilitzar com els dispositius hardware on es realitzaran les còpies. Es definiran les polítiques de rotació de suports per a les diferents tasques de còpia.

Aquest document es revisarà cada dos anys o per incompatibilitats amb els sistemes.

Objectius:

Amb la redacció del document s'aconseguirà un estàndard a les còpies de seguretat de la companyia. Tots els membres del departament d'infraestructures de la informació assignats a la revisió del sistema de backup rebran els logs de les tasques de copia diàriament al seu correu electrònic. S'aconseguirà garantir el correcte funcionament del sistema de còpies mitjançant la recuperació aleatòria de dades. Les còpies de seguretat es guardaran forà de l'oficina central per garantir la seva seguretat.

Afectació

Actius:	Dominis ISO/IEC 27002:2013:
Totes les dades de la companyia.	8. Gestió d'actius. 11. Seguretat física i ambiental. 12. Seguretat a l'operativa. 15. Relacions amb proveïdors.

Riscos mitigats:

Totes les dimensions ACIDA per a les dades i serveis de la companyia.

Durada: 1 mes	**Període de consecució:** Baix

Recursos necessaris	
Personal: - Departament d'infraestructures de la informació. - Responsable de seguretat. - Empresa d'emmagatzematge dels suports de còpia de seguretat.	Econòmic: S'estima un cost intern de 1.000€ en funció de les hores dedicades per personal de la companyia. S'estima un cost de 8.000€ anuals per a la recollida i entrega dels suports.

ID: PRO-009	Continuïtat de les comunicacions externes de la companyia

Descripció:

Es generarà un document amb els procediments a seguir en cas de caiguda del servei de comunicacions de la companyia. S'establiran els diferents backups a les línies de comunicacions i es documentaran totes les connexions existents. Es duplicarà el servidor que dona el servei a la connexió VPN entre els diferents centres i l'accés als usuaris amb teletreball, aquests servidors es trobaran en llocs físics diferents.

Aquest document es revisarà anualment o amb cada canvi a la infraestructura de la xarxa de la companyia.

Objectius:

L'objectiu principal serà evitar la falta de connexió a l'exterior o des de l'exterior. Obtindre un inventari de les diferents adreces IP públiques que disposa la companyia i els serveis que es publiquen per cadascuna d'elles. Protocol·litzar la manera de publicar els serveis per les diferents línies disponibles establint un ordre. Assegurar la interconnexió entre les diferents seus, redundant el servidor VPN de la companyia, així com les connexions dels usuaris de teletreball. Obtindre un document amb les diferents regles dels Firewalls de la companyia que intervenen en la seguretat de les comunicacions.

Afectació

Actius:	Dominis ISO/IEC 27002:2013:
Comunicacions.	6. Aspectes organitzatius de la seguretat de la informació. 13. Seguretat a les telecomunicacions 15. Relacions amb proveïdors. 16. Gestió d'incidents a la seguretat de la informació.

Riscos mitigats:

Totes les dimensions ACIDA per als serveis de la companyia, teletreball, Internet i VPN.

Durada: 1 mes	**Període de consecució:** Baix
Recursos necessaris	
Personal: - Departament d'infraestructures de la informació. - Responsable de seguretat. - Proveïdors de comunicacions. - Proveïdor sistema VPN.	Econòmic: S'estima un cost intern de 1.000€ en funció de les hores dedicades per personal de la companyia. S'estima un cost de 30.000€ anuals per al sistema VPN i les seves línies de connexió.

ID: PRO-010	Pla de formació als usuaris en seguretat de la informació.

Descripció:

S'implantarà un pla de formació per a tota la plantilla, per donar a conèixer el principals requisits del correcte funcionament de la seguretat de la informació, on es donaran les pautes a seguir en cas d'incident de seguretat.

Aquest pla es farà arribar a tot el personal per part del departament de recursos humans i estarà aprovat per la direcció.

Objectius:

L'objectiu principal del pla es aconseguir la correcta formació de la plantilla de la companyia en seguretat de la informació. Minimitzant els riscos de seguretat. Establir pautes per notificar problemes de seguretat detectats pel personal.

Afectació

Actius:	Dominis ISO/IEC 27002:2013:
Tot el personal de la companyia.	7. Seguretat lligada als recursos humans.

Riscos mitigats:

Totes les dimensions ACIDA per a les dades, serveis, xarxa i personal de la companyia.

Durada: 3 mesos	**Període de consecució:** Baix

Recursos necessaris

Personal:	Econòmic:
- Departament d'infraestructures de la informació. - Responsable de seguretat. - Responsable de recursos humans. - Direcció.	S'estima un cost intern de 1.000€ en funció de les hores dedicades per personal de la companyia.

9.10. Annex 10: 114 Controls de la ISO/IEC 27002:2013 actualitzats un cop aplicades les propostes de projectes.

Tot seguit tenim una comparativa dels 114 controls de la ISO/IEC 27002:2013 valorats mitjançant el Model de Maduresa de la Capacitat (CMM) per a l'estat actual de la companyia i un cop aplicades les propostes de projectes:

Dominis	Objectius de control	Controls	CMM Actual	CMM amb projectes aplicats
5. Polítiques de Seguretat				
	5.1. Directrius de la Direcció en seguretat de la informació			
		5.1.1. Conjunt de polítiques per a la seguretat de la informació.	L0	L5
		5.1.2. Revisió de les polítiques per a la seguretat de la informació.	L0	L5
6. Aspectes Organitzatius de la seguretat de la informació				
	6.1. Organització Interna.			
		6.1.1. Assignació de responsabilitats per a la seguretat de la informació.	L2	L2
		6.1.2. Segregació de taques.	L3	L3
		6.1.3. Contacte amb les autoritats.	L3	L3
		6.1.4. Contacte amb els grups d'interès especial.	L2	L2
		6.1.5. Seguretat de la informació a la gestió de projectes.	L5	L5
	6.2. Dispositius per a la mobilitat i el teletreball.			
		6.2.1. Política d'ús de dispositius per a la mobilitat.	L1	L5
		6.2.2. Teletreball.	L2	L4
7. Seguretat lligada als recursos humans.				
	7.1. Abans de la contractació.			
		7.1.1. Investigació d'antecedents.	L2	L2
		7.1.2. Termes i condicions de contractació.	L2	L5

Dominis	Objectius de control	Controls	CMM Actual	CMM amb projectes aplicats
	7.2. Durant la contractació.			
		7.2.1. Responsabilitats de gestió.	L0	L4
		7.2.2. Conscienciació, educació i capacitació en seguretat de la informació.	L0	L5
		7.2.3. Procés disciplinari.	L0	L4
	7.3. Cessament o canvi de lloc de treball.			
		7.3.1. Cessament o canvi de lloc de treball.	L2	L2
8. Gestió d'actius.				
	8.1. Responsabilitat sobre els actius.			
		8.1.1. Inventari d'actius.	L4	L4
		8.1.2. Propietat dels actius.	L4	L4
		8.1.3. Ús acceptable dels actius.	L3	L4
		8.1.4. Devolució d'actius.	L3	L3
	8.2. Classificació de la informació.			
		8.2.1. Directrius de classificació.	L0	L5
		8.2.2. Etiquetatge i manipulació de la informació.	L1	L5
		8.2.3. Manipulació d'actius.	L1	L4
	8.3. Maneig dels suports d'emmagatzematge			
		8.3.1. Gestió de suports extraïbles.	L2	L4
		8.3.2. Eliminació de suports.	L1	L4
		8.3.3. Suports físics en transit.	L1	L4
9. Control d'accés.				
	9.1. Requisits de negoci per al control d'accessos.			
		9.1.1. Política de control d'accessos.	L2	L4
		9.1.2. Control d'accés a les xarxes i serveis associats.	L4	L4
	9.2. Gestió d'accés d'usuari.			
		9.2.1. Gestió d'altes/baixes al registre d'usuaris.	L5	L5
		9.2.2. Gestió dels drets d'accés assignats a usuaris.	L2	L4

Dominis	Objectius de control	Controls	CMM Actual	CMM amb projectes aplicats
		9.2.3. Gestió dels drets d'accés amb privilegis especials.	L2	L2
		9.2.4. Gestió d'informació confidencial d'autenticació d'usuaris.	L4	L4
		9.2.5. Revisió dels drets d'accés dels usuaris.	L2	L4
		9.2.6. Retirada o adaptació dels drets d'accés.	L4	L4
	9.3. Responsabilitats de l'usuari.			
		9.3.1. Ús d'informació confidencial per a l'autenticació.	L1	L5
	9.4. Control d'accés a sistemes i aplicacions.			
		9.4.1. Restricció de l'accés a la informació	L3	L3
		9.4.2. Procediments segurs d'inici de sessió.	L3	L3
		9.4.3. Gestió de contrasenyes d'usuari.	L2	L4
		9.4.4. Ús d'eines d'administració de sistemes.	L1	L4
		9.4.5. Control d'accés al codi font dels programes.	L2	L4
10. Xifratge				
	10.1. Controls criptogràfic.			
		10.1.1. Política d'ús dels controls criptogràfics.	L3	L3
		10.1.2. Gestió de claus.	L0	L0
11. Seguretat física i ambiental.				
	11.1. Àrees segures.			
		11.1.1. Perímetre de seguretat física.	L4	L4
		11.1.2. Controls físics d'entrada.	L4	L4
		11.1.3. Seguretat d'oficines, despatxos i recursos.	L4	L4
		11.1.4. Protecció contra amenaces externes i ambientals.	L4	L4
		11.1.5. El treball en àrees segures.	L4	L4
		11.1.6. Àrees d'accés públic, càrrega i descàrrega.	No aplica	No aplica
	11.2. Seguretat dels			

Dominis	Objectius de control	Controls	CMM Actual	CMM amb projectes aplicats
	equips.			
		11.2.1. Emplaçament i protecció d'equips.	L3	L3
		11.2.2. Instal·lacions de subministre.	L4	L4
		11.2.3. Seguretat del cablejat.	L4	L4
		11.2.4. Manteniment dels equips.	L4	L4
		11.2.5. Sortida d'actius fora de les dependencies de l'empresa.	L4	L4
		11.2.6. Seguretat dels equips i actius fora de les instal·lacions.	L0	L4
		11.2.7. Reutilització o retirada segura de dispositius d'emmagatzematge.	L2	L4
		11.2.8. Equip informàtic d'usuari desatès.	L1	L4
		11.2.9. Política de lloc de treball aclarit i bloqueig de pantalla.	L1	L4
12. Seguretat en la operativa.				
	12.1. Responsabilitats i procediments d'operació.			
		12.1.1. Documentació de procediments d'operació.	L0	L4
		12.1.2. Gestió de canvis.	L3	L4
		12.1.3. Gestió de capacitats.	L3	L3
		12.1.4. Separació d'entorns de desenvolupament, prova i producció.	L2	L2
	12.2. Protecció contra codi maliciós.			
		12.2.1. Controls contra codi maliciós	L4	L4
	12.3. Còpies de seguretat.			
		12.3.1. Còpies de seguretat de la informació.	L4	L5
	12.4. Registre d'activitat i supervisió.			
		12.4.1. Registre i gestió d'esdeveniments d'activitat.	L3	L3
		12.4.2. Protecció dels registres d'informació.	L1	L1
		12.4.3. Registres	L0	L0

Dominis	Objectius de control	Controls	CMM Actual	CMM amb projectes aplicats
		d'activitat de l'administrador i operador del sistema.		
		12.4.4. Sincronització de rellotges.	L5	L5
	12.5. Control del software d'explotació			
		12.5.1. Instal·lació del software a sistemes de producció.	L4	L4
	12.6. Gestió de la vulnerabilitat tècnica.			
		12.6.1. Gestió de les vulnerabilitats tècniques.	L3	L3
		12.6.2. Restriccions a la instal·lació de software.	L0	L5
	12.7. Consideracions de les auditories dels sistemes d'informació.			
		12.7.1. Controls d'auditoria dels sistemes d'informació.	L3	L3
13. Seguretat a les telecomunicacions.				
	13.1. Gestió de la seguretat a les xarxes.			
		13.1.1. Controls de xarxa.	L2	L4
		13.1.2. Mecanismes de seguretat associats a serveis de xarxa.	No aplica	No aplica
		13.1.3. Segregació de xarxes.	L5	L5
	13.2. Intercanvi d'informació amb parts externes.			
		13.2.1. Polítiques i procediments d'intercanvi d'informació.	L4	L5
		13.2.2. Acords d'intercanvi.	L4	L4
		13.2.3. Missatgeria electrònica.	L4	L4
		13.2.4. Acords de confidencialitat i secret.	L3	L3
14. Adquisició, desenvolupament i manteniment dels sistemes d'informació.				
	14.1. Requisits de seguretat dels sistemes d'informació.			

Dominis	Objectius de control	Controls	CMM Actual	CMM amb projectes aplicats
		14.1.1. Anàlisi i especificació dels requisits de seguretat.	L2	L4
		14.1.2. Seguretat de les comunicacions en serveis accessibles per xarxes públiques.	L3	L3
		14.1.3. Protecció de les transaccions per xarxes telemàtiques.	L4	L4
	14.2. Seguretat als processos de desenvolupament i suport.			
		14.2.1. Política de desenvolupament segur de software.	L3	L3
		14.2.2. Procediments de control de canvis als sistemes.	L2	L2
		14.2.3. Revisió tècnica de les aplicacions després d'efectuar canvis al sistema operatiu.	L2	L2
		14.2.4. Restriccions als canvis en els paquets de software.	L2	L2
		14.2.5. Ús de principis d'enginyeria en protecció de sistemes.	L2	L2
		14.2.6. Seguretat en entorns de desenvolupament.	L1	L1
		14.2.7. Externalització del desenvolupament de software.	L5	L5
		14.2.8. Proves de funcionalitat durant el desenvolupament dels sistemes.	L4	L4
		14.2.9. Proves d'acceptació.	L3	L3
	14.3. Dades de prova.			
		14.3.1. Protecció de les dades utilitzades en proves.	L5	L5
15. Relacions amb subministradors.				
	15.1. Seguretat de la informació a les relacions amb subministradors.			
		15.1.1. Política de seguretat de la informació per a subministradors.	L4	L4
		15.1.2. Tractament del risc dintre dels acords de subministradors.	L3	L4

Dominis	Objectius de control	Controls	CMM Actual	CMM amb projectes aplicats
		15.1.3. Cadena de subministrament en tecnologies de la informació i comunicacions.	L2	L2
	15.2. Gestió de la prestació del servei per subministradors.			
		15.2.1. Supervisió i revisió del serveis prestats per tercers.	L1	L3
		15.2.2. Gestió de canvis als serveis prestats per tercers.	L3	L3
16. Gestió d'incidents a la seguretat de la informació.				
	16.1. Gestió d'incidents de seguretat de la informació i millores.			
		16.1.1. Responsabilitats i procediments.	L2	L4
		16.1.2. Notificació dels esdeveniments de seguretat de la informació.	L4	L4
		16.1.3. Notificació de punts dèbils de la seguretat.	L4	L4
		16.1.4. Valoració d'esdeveniments de seguretat de la informació i presa de decisions.	L2	L3
		16.1.5. Resposta als incidents de seguretat.	L2	L4
		16.1.6. Aprenentatge dels incidents de seguretat de la informació.	L2	L2
		16.1.7. Recopilació d'evidències.	L1	L1
17. Aspectes de seguretat de la informació a la gestió de la continuïtat del negoci.				
	17.1. Continuïtat de la seguretat de la informació.			
		17.1.1. Planificació de la continuïtat de la seguretat de la informació.	L4	L4
		17.1.2. Implantació de la continuïtat de la seguretat de la informació.	L1	L4
		17.1.3. Verificació,	L3	L4

Dominis	Objectius de control	Controls	CMM Actual	CMM amb projectes aplicats
		revisió i avaluació de la continuïtat de la seguretat de la informació.		
	17.2. Redundàncies.			
		17.2.1. Disponibilitat d'instal·lacions per al processament de la informació.	L5	L5
18. Compliment.				
	18.1. Compliment dels requisits legals i contractuals.			
		18.1.1. Identificació de la legislació aplicable.	L3	L3
		18.1.2. Drets de propietat intel·lectual (DPI).	L4	L4
		18.1.3. Protecció dels registres de l'organització.	L4	L4
		18.1.4. Protecció de dades i privacitat de la informació personal.	L3	L3
		18.1.5. Regulació dels controls criptogràfics.	L3	L3
	18.2. Revisions de la seguretat de la informació.			
		18.2.1. Revisió independent de la seguretat de la informació.	L4	L4
		18.2.2. Compliment de les polítiques i normes de seguretat.	L2	L4
		18.2.3. Comprovació del compliment.	L2	L4

Taula 20: Comparativa dels 114 Controls de la ISO/IEC 27002:2013 un cop aplicades les propostes de projectes.

9.11. Annex 11: Taula comparativa de l'impacte potencial abans i després d'aplicar els projectes.

La següent taula s'ha calculat amb el full d'Excel "Calcul_ImpactePotencial_Risc_Projectes.xlsx" full Impacte_Potencial_Projectes adjunt.

Àmbit	Actiu	Aspectes crítics					Impacte màxim amenaça després de projectes					Impacte potencial					Impacte potencial després de projectes				
		A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
Instal·lacions																					
	Oficines centrals de la companyia	9	9	9	9	8		5%	5%	25%			0.45	1.35	9			0.45	0.45	2.25	
Hardware																					
	Servidor de correu	8	8	8	8	8		25%	25%	30%			6	6	8			2	2	2.4	
	Servidor Web	6	6	6	5	5		25%	25%	30%			4.5	4.5	5			1.5	1.5	1.5	
	Servidor d'antivirus	6	4	4	3	4		25%	25%	30%			2	1	3			1	1	0.9	
	Controlador de domini principal	7	7	6	4	6		25%	25%	30%			5.25	4.5	4			1.75	1.5	1.2	
	Controlador de domini secundari	7	7	5	3	5		25%	25%	30%			3.5	1.25	3			1.75	1.25	0.9	
	Firewall	6	6	5	5	6		25%	25%	30%			4.5	3.75	5			1.5	1.25	1.5	
	Servidor de còpies de seguretat	5	5	4	4	4		25%	25%	30%			2.5	1	4			1.25	1	1.2	
	Servidor CRM	8	8	8	8	8		25%	25%	30%			6	6	8			2	2	2.4	
	Servidor de base de dades	7	7	7	7	6		25%	25%	30%			5.25	5.25	7			1.75	1.75	2.1	
	Servidor de dades	8	8	8	8	4		25%	25%	30%			6	6	8			2	2	2.4	
	NAS	8	8	8	8	2		25%	25%	30%			6	6	8			2	2	2.4	
	Servidors de desenvolupament	4	1	1	1	1		25%	5%	30%			0.25	0.05	1			0.25	0.05	0.3	
	Switches CPD	8	8	8	8	2		25%	25%	30%			6	6	8			2	2	2.4	
	Switches	4	2	4	4	1		25%	15%	30%			1	1	4			0.5	0.6	1.2	
	Routers	6	2	5	6	3		25%	25%	30%			1.5	3.75	6			0.5	1.25	1.8	
	Servidor Navision Dynamics	8	8	8	8	8		25%	25%	30%			6	6	8			2	2	2.4	
	Controlador de domini secundari al núvol	7	7	5	2	5		15%	5%	30%			3.5	1.25	2			1.05	0.25	0.6	

Àmbit	Actiu	Aspectes crítics					Impacte màxim amenaça després de projectes					Impacte potencial					Impacte potencial després de projectes				
		A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
	Portàtils tècnics	6	5	2	2	1		15%	5%	30%			2.5	0.5	2			0.75	0.1	0.6	
	Portàtils no tècnics	6	5	2	2	1		15%	5%	30%			2.5	0.5	2			0.75	0.1	0.6	
	Equips sobretaula tècnics	6	5	2	2	1		15%	5%	30%			2.5	0.5	2			0.75	0.1	0.6	
	Equips sobretaula no tècnics	6	5	2	2	1		15%	5%	30%			2.5	0.5	2			0.75	0.1	0.6	
	Multifuncionals A3/A4 color	4	2	2	4	1		10%	5%	30%			0.5	0.1	4			0.2	0.1	1.2	
	Plotters	4	2	4	4	1		15%	5%	30%			0.5	0.2	4			0.3	0.2	1.2	
	Mòbils	4	4	2	3	1		15%	5%	30%			1	0.1	3			0.6	0.1	0.9	
	Telèfons fixes	3	2	2	2	0		15%	5%	30%			0.5	0.1	2			0.3	0.1	0.6	
	Centraleta de telefonia IP	6	6	5	6	2		25%	25%	30%			4.5	3.75	6			1.5	1.25	1.8	
Aplicació																					
	Microsoft Exchange Server	8	8	8	8	8	5%	5%	5%	30%		2	6	6	8		0.4	0.4	0.4	2.4	
	Microsoft SharePoint Server	7	7	6	4	6	10%	15%	15%	20%		3.15	3.15	2.7	1.6		0.7	1.05	0.9	0.8	
	ePO McAfee	5	4	5	3	4	5%	25%	25%	25%		1.25	2	2.5	1.5		0.25	1	1.25	0.75	
	Aplicació pròpia d'inventari	6	4	2	2	1	15%	15%	15%	20%		2.7	1.8	0.9	0.8		0.9	0.6	0.3	0.4	
	Aplicació pròpia d'alta i baixa d'usuaris	6	6	2	2	1	15%	15%	15%	20%		2.7	2.7	0.9	0.8		0.9	0.9	0.3	0.4	
	Aplicació pròpia d'inventari de mòbils	6	4	2	2	1	15%	15%	15%	20%		2.7	1.8	0.9	0.8		0.9	0.6	0.3	0.4	
	Microsoft Windows Server	8	4	6	7	2	5%	25%	25%	30%		2	3	4.5	7		0.4	1	1.5	2.1	
	Microsoft ISA Server	8	4	5	8	6	5%	15%	15%	20%		2	2	2.5	4		0.4	0.6	0.75	1.6	
	Symantec BackupExec	8	2	2	2	3	15%	25%	25%	25%		3.6	0.9	0.9	0.8		1.2	0.5	0.5	0.5	
	Microsoft CRM	8	8	8	8	8	5%	25%	25%	30%		2	6	6	8		0.4	2	2	2.4	
	Microsoft Navision Dynamics	8	8	8	8	8	5%	25%	25%	30%		2	6	6	8		0.4	2	2	2.4	
	Microsoft Windows	6	2	5	5	2	5%	15%	15%	15%		1.5	1	2.5	2.5		0.3	0.3	0.75	0.75	
	Microsoft Office	6	1	3	3	1	15%	15%	15%	15%		2.7	0.45	1.35	1.20		0.9	0.15	0.45	0.45	
	Gestió d'incidències	6	1	2	2	3	15%	15%	15%	15%		2.7	0.45	0.9	0.8		0.9	0.15	0.3	0.3	
	Aplicacions de càlcul	7	6	6	4	1	5%	15%	15%	15%		1.75	3	3	2		0.35	0.9	0.9	0.6	

Àmbit	Actiu	Aspectes crítics					Impacte màxim amenaça després de projectes					Impacte potencial					Impacte potencial després de projectes				
		A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
	Aplicacions de disseny	7	6	6	4	1	5%	15%	15%	15%		1.75	3	3	2		0.35	0.9	0.9	0.6	
Dades																					
	Projectes propis	10	10	10	10	10	15%	25%	30%	30%		6.5	8	9	9		1.5	2.5	3	3	
	Base de dades CRM	10	10	10	10	10	15%	25%	30%	30%		6.5	8	9	9		1.5	2.5	3	3	
	Base de dades de personal	7	9	8	6	4	15%	25%	30%	30%		4.55	7.2	7.2	5.4		1.05	2.25	2.4	1.8	
	Base de dades Navision Dynamics	8	8	8	8	7	15%	25%	30%	30%		5.2	6.4	7.2	6.3		1.2	2	2.4	2.4	
	Codi font aplicació pròpia d'inventari	7	8	8	5	2	5%	15%	15%	15%		0.35	4	4	2.5		0.35	1.2	1.2	0.75	
	Codi font aplicació pròpia d'alta i baixa d'usuaris	7	8	8	5	2	5%	15%	15%	15%		0.35	4	4	2.5		0.35	1.2	1.2	0.75	
	Codi font aplicació pròpia d'inventari de mòbils	7	8	8	5	2	5%	15%	15%	15%		0.35	4	4	2.5		0.35	1.2	1.2	0.75	
Xarxa																					
	Línies RTB	8	1	1	5	0		5%	5%	25%			0.05	0.05	3.75			0.05	0.05	1.25	
	Línies RDSI	8	7	8	8	1		5%	5%	45%			0.35	0.40	6.8			0.35	0.4	3.6	
	Internet fibra òptica	8	8	8	8	6	15%	30%	30%	50%		4	6.4	4.80	7.2		1.2	1.2	1.2	2.4	
	LAN	8	8	8	8	8	15%	30%	30%	40%		4	6.4	4.8	7.2		1.2	1.2	1.2	2.4	
	VPN	8	8	7	6	7	15%	40%	30%	40%		4	6.4	4.2	5.4		1.2	1.2	0.7	1.2	
Serveis																					
	Correu electrònic	9	9	9	9	7	15%	25%	25%	40%		4.5	6.75	6.75	8.1		1.35	2.25	2.25	2.7	
	Intranet	8	6	5	3	3	15%	25%	25%	40%		4	4.5	3.75	2.7		1.2	1.5	1.25	0.9	
	Emmagatzematge de dades	9	9	9	9	8	15%	25%	25%	40%		4.5	6.75	6.75	8.1		1.35	2.25	2.25	2.7	
	Teletreball	8	8	6	3	3	15%	25%	25%	40%		4	6	4.5	2.7		1.2	2	1.5	1.2	
Equipament auxiliar																					
	Racks de servidors	3	1	1	1	0		5%	5%	50%			0.1	0.1	1			0.05	0.05	0.5	
	Racks de comunicacions	3	1	1	1	0		10%	10%	50%			0.1	0.1	1			0.1	0.1	0.5	
	SAI	6	3	8	8	1		15%	15%	50%			0.75	2	8			0.45	1.2	4	
	Generador elèctric a gasoil	6	3	7	7	1		15%	15%	50%			0.75	1.75	7			0.45	1.05	3.5	

Àmbit	Actiu	Aspectes crítics					Impacte màxim amenaça després de projectes					Impacte potencial					Impacte potencial després de projectes				
		A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
	Climatització	8	3	8	9	1		15%	15%	50%			0.75	2	9			0.45	1.2	4.5	
	Climatització de reserva	8	3	7	7	1		15%	15%	50%			0.75	1.75	7			0.45	1.05	3.5	
	Control d'accés	8	6	7	3	1		15%	15%	50%			1.5	1.75	3			0.9	1.05	1.5	
	Càmeres de vigilància	6	5	4	3	1		15%	15%	50%			1.25	1	3			0.75	0.6	1.5	
	Sensors elèctrics i ambientals	5	1	4	4	1		15%	15%	50%			0.25	1	4			0.15	0.6	2	
Personal																					
	Usuaris interns	10	9	10	10	9		25%	15%	10%			6.75	5	1			2.25	1.5	1	
	Administradors de sistemes	10	10	10	10	10		25%	15%	10%			7.5	5	1			2.5	1.5	1	
	Programadors	10	10	9	6	8		25%	15%	10%			7.5	4.5	0.6			2.5	1.35	0.6	
	Proveïdors	10	10	10	7	8		10%	10%	10%			1.5	1.5	0.7			1	1	0.7	

Taula 21: Taula comparativa de l'impacte potencial abans i després d'aplicar els projectes.

9.12. Annex 12: Taula comparativa del nivell de risc abans i després d'aplicar els projectes.

La següent taula s'ha calculat amb el full d'Excel "Calcul_ImpactePotencial_Risc_Projectes.xlsx" full Calcul_Risc_Projectes adjunt.

Podem veure marcat en color groc totes les dimensions dels actius que superen el risc acceptable per la companyia.

Àmbit	Actiu	Freq.	Impacte potencial					Impacte potencial després de projectes					Risc					Risc després de projectes				
			A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
Instal·lacions																						
	Oficines centrals de la companyia	1		0.45	1.35	9			0.45	0.45	2.25			0.45	1.35	9			0.45	0.45	2.25	
Hardware																						
	Servidor de correu	3		6	6	8			2	2	2.4			18	18	24			6	6	7.2	
	Servidor Web	3		4.5	4.5	5			1.5	1.5	1.5			13.5	13.5	15			4.5	4.5	4.5	
	Servidor d'antivirus	3		2	1	3			1	1	0.9			6	3	9			3	3	2.7	
	Controlador de domini principal	5		5.25	4.5	4			1.75	1.5	1.2			26.25	22.5	20			8.75	7.5	6	
	Controlador de domini secundari	5		3.5	1.25	3			1.75	1.25	0.9			17.5	6.25	15			8.75	6.25	4.5	
	Firewall	3		4.5	3.75	5			1.5	1.25	1.5			13.5	22.5	15			4.5	3.75	4.5	
	Servidor de còpies de seguretat	5		2.5	1	4			1.25	1	1.2			12.5	5	20			6.25	5	6	
	Servidor CRM	3		6	6	8			2	2	2.4			18	18	24			6	6	7.2	
	Servidor de base de dades	3		5.25	5.25	7			1.75	1.75	2.1			15.75	15.75	21			5.25	5.25	6.3	
	Servidor de dades	3		6	6	8			2	2	2.4			18	18	24			6	6	7.2	
	NAS	3		6	6	8			2	2	2.4			18	18	24			6	6	7.2	
	Servidors de desenvolupament	4		0.25	0.05	1			0.25	0.05	0.3			1	0.20	4			1	0.2	1.2	
	Switches CPD	3		6	6	8			2	2	2.4			18	18	24			6	6	7.2	
	Switches	5		1	1	4			0.5	0.6	1.2			5	5	20			2.5	3	6	
	Routers	3		1.5	3.75	6			0.5	1.25	1.8			4.5	11.25	18			1.5	3.75	5.4	
	Servidor Navision Dynamics	3		6	6	8			2	2	2.4			18	18	24			6	6	7.2	

Àmbit	Actiu	Freq.	Impacte potencial					Impacte potencial després de projectes					Risc					Risc després de projectes				
			A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
	Controlador de domini secundari al núvol	5		3.5	1.25	2			1.05	0.25	0.6			17.5	6.25	10			5.25	1.25	3	
	Portàtils tècnics	5		2.5	0.5	2			0.75	0.1	0.6			12.5	2.5	10			3.75	0.5	3	
	Portàtils no tècnics	5		2.5	0.5	2			0.75	0.1	0.6			12.5	2.5	10			3.75	0.5	3	
	Equips sobretaula tècnics	5		2.5	0.5	2			0.75	0.1	0.6			12.5	2.5	10			3.75	0.5	3	
	Equips sobretaula no tècnics	5		2.5	0.5	2			0.75	0.1	0.6			12.5	2.5	10			3.75	0.5	3	
	Multifuncionals A3/A4 color	4		0.5	0.1	4			0.2	0.1	1.2			2	0.4	16			0.8	0.4	4.8	
	Plotters	4		0.5	0.2	4			0.3	0.2	1.2			2	0.8	16			1.2	0.8	4.8	
	Mòbils	4		1	0.1	3			0.6	0.1	0.9			4	0.4	12			2.4	0.4	3.6	
	Telèfons fixes	4		0.5	0.1	2			0.3	0.1	0.6			2	0.4	8			1.2	0.4	2.4	
	Centraleta de telefonia IP	3		4.5	3.75	6			1.5	1.25	1.8			13.5	11.25	18			4.5	3.75	5.4	
Aplicació																						
	Microsoft Exchange Server	4	2	6	6	8		0.4	0.4	0.4	2.4		8	24	24	32		1.6	1.6	1.6	9.6	
	Microsoft SharePoint Server	1	3.15	3.15	2.7	1.6		0.7	1.05	0.9	0.8		3.15	3.15	2.7	1.6		0.7	10.5	0.9	0.8	
	ePO McAfee	4	1.25	2	2.5	1.5		0.25	1	1.25	0.75		5	8	10	6		1	4	5	3	
	Aplicació pròpia d'inventari	1	2.7	1.8	0.9	0.8		0.9	0.6	0.3	0.4		2.7	1.8	0.9	0.8		0.9	0.6	0.3	0.4	
	Aplicació pròpia d'alta i baixa d'usuaris	1	2.7	2.7	0.9	0.8		0.9	0.9	0.3	0.4		2.7	2.7	0.9	0.8		0.9	0.9	0.3	0.4	
	Aplicació pròpia d'inventari de mòbils	1	2.7	1.8	0.9	0.8		0.9	0.6	0.3	0.4		2.7	1.8	0.9	0.8		0.9	0.6	0.3	0.4	
	Microsoft Windows Server	4	2	3	4.5	7		0.4	1	1.5	2.1		8	12	18	28		1.6	4	6	8.4	
	Microsoft ISA Server	4	2	2	2.5	4		0.4	0.6	0.75	1.6		8	4	10	16		1.6	2.4	3	6.4	
	Symantec BackupExec	1	3.6	0.9	0.9	0.8		1.2	0.5	0.5	0.5		3.6	0.9	0.9	0.8		1.2	0.5	0.5	0.5	

Àmbit	Actiu	Freq.	Impacte potencial					Impacte potencial després de projectes					Risc					Risc després de projectes				
			A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
	Microsoft CRM	4	2	6	6	8		0.4	2	2	2.4		8	24	24	32		1.6	8	8	9.6	
	Microsoft Navision Dynamics	4	2	6	6	8		0.4	2	2	2.4		8	24	24	32		1.6	8	8	9.6	
	Microsoft Windows	4	1.5	1	2.5	2.5		0.3	0.3	0.75	0.75		6	4	10	10		1.2	1.2	3	3	
	Microsoft Office	1	2.7	0.45	1.35	1.20		0.9	0.15	0.45	0.45		2.7	0.45	1.35	1.20		0.9	0.15	0.45	0.45	
	Gestió d'incidències	1	2.7	0.45	0.9	0.8		0.9	0.15	0.3	0.3		2.7	0.45	0.9	0.8		0.9	0.15	0.3	0.3	
	Aplicacions de càlcul	4	1.75	3	3	2		0.35	0.9	0.9	0.6		7	12	12	8		1.4	3.6	3.6	2.4	
	Aplicacions de disseny	4	1.75	3	3	2		0.35	0.9	0.9	0.6		7	12	12	8		1.4	3.6	3.6	2.4	
Dades																						
	Projectes propis	5	6.5	8	9	9		1.5	2.5	3	3		32.5	40	45	45		7.5	12.5	15	15	
	Base de dades CRM	1	6.5	8	9	9		1.5	2.5	3	3		6.5	8	9	9		1.5	2.5	3	3	
	Base de dades de personal	5	4.55	7.2	7.2	5.4		1.05	2.25	2.4	1.8		22.75	36	36	27		5.25	11.25	12	9	
	Base de dades Navision Dynamics	5	5.2	6.4	7.2	6.3		1.2	2	2.4	2.4		26	32	36	31.5		6	10	12	12	
	Codi font aplicació pròpia d'inventari	1	0.35	4	4	2.5		0.35	1.2	1.2	0.75		0.35	4	4	2.5		0.35	1.2	1.2	0.75	
	Codi font aplicació pròpia d'alta i baixa d'usuaris	1	0.35	4	4	2.5		0.35	1.2	1.2	0.75		0.35	4	4	2.5		0.35	1.2	1.2	0.75	
	Codi font aplicació pròpia d'inventari de mòbils	1	0.35	4	4	2.5		0.35	1.2	1.2	0.75		0.35	4	4	2.5		0.35	1.2	1.2	0.75	
Xarxa																						
	Línies RTB	1		0.05	0.05	3.75			0.05	0.05	1.25			0.05	0.05	3.75			0.05	0.05	1.25	
	Línies RDSI	10		0.35	0.40	6.8			0.35	0.4	3.6			3.5	4	68			3.5	4	24	
	Internet fibra òptica	10	4	6.4	4.80	7.2		1.2	2.4	2.4	4		40	64	48	72		12	12	12	24	
	LAN	10	4	6.4	4.8	7.2		1.2	2.4	2.4	3.2		40	64	48	72		12	12	12	24	
	VPN	10	4	6.4	4.2	5.4		1.2	3.2	2.1	2.4		40	64	42	54		12	12	7	12	
Serveis																						
	Correu electrònic	7	4.5	6.75	6.75	8.1		1.35	2.25	2.25	3.6		31.5	47.25	47.25	56.7		9.45	15.75	15.75	18.9	
	Intranet	7	4	4.5	3.75	2.7		1.2	1.5	1.25	1.2		28	31.5	26.25	18.9		8.4	10.5	8.75	6.3	
	Emmagatzematge	7	4.5	6.75	6.75	8.1		1.35	2.25	2.25	3.6		31.5	47.25	47.25	56.7		9.45	15.75	15.75	18.9	

Àmbit	Actiu	Freq.	Impacte potencial					Impacte potencial després de projectes					Risc					Risc després de projectes				
			A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
	de dades																					
	Teletreball	7	4	6	4.5	2.7		1.2	2	1.5	1.2		28	42	31.5	18.9		8.4	14	10.5	8.4	
Equipament auxiliar																						
	Racks de servidors	1		0.1	0.1	1			0.05	0.05	0.5			0.1	0.1	1			0.05	0.05	0.5	
	Racks de comunicacions	1		0.1	0.1	1			0.1	0.1	0.5			0.1	0.1	1			0.1	0.1	0.5	
	SAI	1		0.75	2	8			0.45	1.2	4			0.75	2	8			0.45	1.2	4	
	Generador elèctric a gasoil	1		0.75	1.75	7			0.45	1.05	3.5			0.75	1.75	7			0.45	1.05	3.5	
	Climatització	1		0.75	2	9			0.45	1.2	4.5			0.75	2	9			0.45	1.2	4.5	
	Climatització de reserva	1		0.75	1.75	7			0.45	1.05	3.5			0.75	1.75	7			0.45	1.05	3.5	
	Control d'accés	1		1.5	1.75	3			0.9	1.05	1.5			1.5	1.75	3			0.9	1.05	1.5	
	Càmeres de vigilància	1		1.25	1	3			0.75	0.6	1.5			1.25	1	3			0.75	0.6	1.5	
	Sensors elèctrics i ambientals	1		0.25	1	4			0.15	0.6	2			0.25	1	4			0.15	0.6	2	
Personal																						
	Usuaris interns	5		6.75	5	1			2.25	1.5	1			33.75	25	5			11.25	7.5	5	
	Administradors de sistemes	5		7.5	5	1			2.5	1.5	1			37.5	25	5			12.5	7.5	5	
	Programadors	5		7.5	4.5	0.6			2.5	1.35	0.6			37.5	22.5	3			12.5	6.75	3	
	Proveidors	4		1.5	1.5	0.7			1	1	0.7			6	6	2.8			4	4	2.8	

Taula 22: Taula comparativa del nivell de risc abans i després d'aplicar els projectes.

9.13. Annex 13: Informe d'auditoria de compliment.

Títol: **Auditoria de Compliment**	Elaborat per: Jsanchezce Data: 04/06/2016	Versió: 1	Revisat per: Data:

Índex:

Objectiu:

Amb l'auditoria de compliment s'ha de verificar el compliment dels 114 controls continguts en 14 dominis de la norma ISO/IEC 27002:2013 i avaluar el seu estat de maduresa en aplicar el sistema SGSI de l'empresa INGENSA, S.L..

Abast:

L'auditoria de compliment afectarà a tots els actius de la companyia, als diferents departaments, informes d'auditories prèvies i al SGSI amb tota la seva documentació relacionada i aportada per INGENSA, S.L. a la seva seu central a Madrid.

Equip auditor:

L'equip auditor estarà format per els següents membres de l'empresa d'auditories AUDITUOC, S.L. un cop signat el contracte de confidencialitat:

- Auditor en cap.
- Dos experts tècnics expecialistes en les següents mateires:
    - Expert 1:
        - Polítiques de seguretat.

        - Organització de la seguretat.
        - Gestió d'actius.
        - Gestió d'incidents.
    - Expert 2:
        - Gestió de RRHH.
        - Continuïtat de negoci.
        - Compliment legal.
        - Protecció física i del entorn.

Documentació de referència:

Per dur a terme l'auditoria de compliment s'ha fet servir la següent documentació oficial:

- ISO/IEC 27001.
- ISO/IEC 27002.
- Model de Maduresa de la Capacitat (CMM).
- MAGERIT v.3.0.

Metodologia emprada:

El procés d'auditoria de compliment s'ha realitzat mitjançant l'avaluació del compliment dels controls de la norma ISO/IEC 27002:2013 utilitzant el Model de Maduresa de la Capacitat (CMM).

Procediment i control de proves:

La documentació revisada en aquesta auditoria ha estat la següent:

- Política de seguretat d'INGENSA, S.L.: s'ha revisat la definició de seguretat, s'ha comprovat el suport de la direcció a la implantació del SGSI i s'ha verificat l'existència dels diferents rols i responsabilitats.
- Anàlisi de riscos: s'ha verificat l'anàlisi de riscos documentat per la companyia mitjançant MAGERIT v.3.
- Compliment dels 114 controls ISO/IEC 27002:2013: s'ha realitzat un anàlisi de compliment dels 114 controls de la norma ISO/IEC 27002:2013, així com l'avaluació el seu estat de maduresa

mitjançant el model de maduresa de la capacitat (CMM), partint de l'estat inicial documentat al SGSI. El resultat d'aquest anàlisi el podem veure a la taula de l'annex I.

Resum executiu:

S'ha realitzat una auditoria de primera part de l'SGSI de l'empresa INGENSA, S.L., on s'ha comprovat el compliment dels diferents controls de la norma ISO/IEC 27002:2013 i el seu estat de maduresa. Aquest tipus d'auditoria es realitza amb tota la informació necessària aportada per la empresa. L'auditoria es realitza sobre la seu central de la companyia a Madrid.

S'ha realitzat una verificació de la documentació del SGSI exigida a la norma ISO/IEC 27001, un compliment dels controls ISO/IEC 27002:2013, un estat de maduresa segons el model de maduresa de la capacitat (CMM) i una comprovació de l'anàlisi de riscos realitzat segons MAGERIT v.3

Un cop realitzats els anàlisis, es documenten 8 no conformitats, 7 d'elles menors i 1 major. Que afecten a diferents dominis de seguretat de la norma ISO/IEC 27002:2013 i relacionades amb els controls que es troben en un estat de maduresa inicial o inexistent.

Les recomanacions que s'haurien de dur a terme, passen per realitzar les accions correctores indicades a cadascuna de les no conformitats adjuntades a aquest informe:

- NC-01: Seguretat lligada als recursos humans.
- NC-02: Gestió d'actius.
- NC-03: Control d'accés.
- NC-04: Xifratge.
- NC-05: Seguretat en la operativa.
- NC-06: Adquisició, desenvolupament i manteniment dels sistemes d'informació.
- NC-07: Relacions amb subministradors.
- NC-08: Gestió d'incidents a la seguretat de la informació.

No conformitats:

A continuació podem veure el llistat de les diferents no conformitats trobades amb l'execució de l'auditoria de compliment:

<table>
<tr><td>ID: NC-01</td><td>Data obertura: 26/05/2016</td><td>Data fi:</td></tr>
<tr><td colspan="3">Descripció:
Quan s'ha de realitzar un canvi en el lloc de treball d'un empleat, no s'està duent a terme el procediment com es troba documentat.</td></tr>
<tr><td colspan="3">Tipus: ☐ Major ☒ Menor</td></tr>
<tr><td colspan="3">Afectació ISO/IEC 27002:2013</td></tr>
<tr><td colspan="2">Controls:
7.3.1. Cessament o canvi del lloc de treball.</td><td>Dominis:
7. Seguretat lligada als recursos humans.</td></tr>
<tr><td colspan="3">Acció correctora:
Es realitzaran revisions periòdiques per a assegurar-nos de la correcta aplicació del procediment i així aconseguir una comunicació fluida i eficaç entre els departaments afectats per dur a terme aquests canvis de lloc de treball.</td></tr>
<tr><td colspan="3">Responsable assignat: Responsable de RRHH i responsable de seguretat.</td></tr>
</table>

ID: NC-02	Data obertura: 26/05/2016	Data fi:

Descripció:

Encara que la companyia disposa d'una utilitat pròpia per a la gestió dels actius, existeixen actius que no es troben assignats a cap usuari o responsable de departament.

Tipus: ☐ Major ☒ Menor

Afectació ISO/IEC 27002:2013

Controls:	Dominis:
8.1.2. Propietat dels actius.	8. Gestió d'actius.

Acció correctora:

Es revisarà la utilitat d'inventari de la companyia per assignar tots els actius als seus usuaris i en el cas de ser un equip genèric, aquest s'assignarà al responsable del departament propietari.

Responsable assignat: Responsable del departament d'Infraestructura de la informació.

ID: NC-03	Data obertura: 26/05/2016	Data fi:

Descripció:

Encara que les accessos es sol·liciten mitjançant incidència per part del responsable del departament afectat i es troben restringits en funció del nivell o de les necessitats dels usuaris, aquests accessos no es troben documentats.

Tipus: ☐ Major ☒ Menor

Afectació ISO/IEC 27002:2013

Controls:	Dominis:
9.2.3. Gestió dels drets d'accés amb privilegis especials. 9.4.1. Restricció d'accés a la informació.	9. Control d'accés.

Acció correctora:

S'han de realitzar revisions periòdiques dels diferents accessos que disposen els usuaris i s'ha de mantindre un document amb aquest llistat d'accessos actualitzats.

Responsable assignat: Responsables dels departaments i Departament d'Infraestructures de la informació.

ID: NC-04	Data obertura: 26/05/2016	Data fi:

Descripció:

No existeix cap política per a la gestió i control de les claus criptogràfiques.

Tipus: ☐ Major ☒ Menor

Afectació ISO/IEC 27002:2013

Controls:	Dominis:
10.1.2. Gestió de claus.	10. Xifratge.

Acció correctora:

S'ha de procedir amb la redacció d'una política de seguretat per a l'ús, protecció i cicle de vida de les claus criptogràfiques.

Responsable assignat: Responsable de seguretat.

ID: NC-05	Data obertura: 26/05/2016	Data fi:

Descripció:

Encara que hi ha definida una política per al tractament dels logs dels sistemes i de l'activitat dels administradors. Aquesta informació no es troba assegurada, no es revisa amb freqüència i l'activitat dels administradors no queda enregistrada en la seva totalitat.

Tipus: ☒ Major ☐ Menor

Afectació ISO/IEC 27002:2013

Controls:	Dominis:
12.4.2. Protecció dels registres d'informació. 12.4.3. Registres d'activitat de l'administrador i operador del sistema.	12. Seguretat en la operativa.

Acció correctora:

S'ha de garantir el correcte compliment de la política de seguretat de logs definida al SGSI de la companyia.

Responsable assignat: Responsable departament d'Infraestructura de la Informació.

ID: NC-06	Data obertura: 26/05/2016	Data fi:

Descripció:

No existeix cap política per al control de canvis als sistemes, encara que aquests es realitzen per personal del departament d'infraestructures de la informació. Tampoc existeix cap política que especifiqui el nivell de seguretat que han de tindre els entorns de desenvolupament.

Tipus: ☐ Major ☒ Menor

Afectació ISO/IEC 27002:2013

Controls:	Dominis:
14.2.2. Procediments de control de canvis als sistemes. 14.2.6. Seguretat en entorns de desenvolupament.	14. Adquisició, desenvolupament i manteniment dels sistemes d'informació.

Acció correctora:

S'ha de crear una política per a protocol·litzar el procediment de canvis als sistemes i documentar tots els canvis que es realitzin. Així mateix, a la mateixa política de seguretat es definiran les necessitats de seguretat que han de tindre els entorns de desenvolupament, ja que ara mateix no disposen de cap tipus de control.

Responsable assignat: Responsable departament d'infraestructures de la informació i responsable de seguretat.

ID: NC-07	Data obertura: 26/05/2016	Data fi:

Descripció:

Un cop revisats tots els LSA dels diferents proveïdors, trobem que la companyia no disposa de tots els acords de serveis.

Tipus: ☐ Major ☒ Menor

Afectació ISO/IEC 27002:2013

Controls:	Dominis:
15.1.3. Cadena de subministrament en tecnologies de la informació i comunicacions.	15. Relacions amb subministradors.

Acció correctora:

S'hauran de revisar els diferents acords de serveis dels proveïdors i contactar amb els que no ens han proporcionat la còpia del mateix i arxivar-la.

Responsable assignat: Responsable departament d'infraestructures de la informació.

ID: NC-08	Data obertura: 26/05/2016	Data fi:

Descripció:

Encara que existeix una política de seguretat per a la gestió d'incidents, actualment la companyia no disposa de cap base de coneixement ni està recopilant i preservant les dades que podrien servir com a evidències.

Tipus: ☐ Major ☒ Menor

Afectació ISO/IEC 27002:2013

Controls:	Dominis:
16.1.6. Aprenentatge dels incidents de seguretat de la informació. 16.1.7. Recopilació d'evidències.	16. Gestió d'incidents a la seguretat de la informació.

Acció correctora:

Es realitza un calendari per a tornar a revisar l'aplicació de la política de seguretat per a la gestió d'incidents i comprovar el correcte compliment dels controls.

Responsable assignat: Responsable departament d'infraestructura de la informació i responsable de seguretat.

Annexos:

Annex I: Compliment dels 114 Controls de la ISO/IEC 27002:2013 actualitzats un cop aplicades les propostes de projectes.

Tot seguit tenim taula de compliment dels 114 controls de la norma ISO/IEC 27002:2013 amb el seu estat de maduresa seguint el Model de Maduresa de la Capacitat (CMM) i indicant si compleix amb la norma:

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
5. Polítiques de Seguretat					
	5.1. Directrius de la Direcció en seguretat de la informació				
		5.1.1. Conjunt de polítiques per a la seguretat de la informació.	L5	SI	Existeix una política de seguretat aprovada per la direcció.
		5.1.2. Revisió de les polítiques per a la seguretat de la informació.	L5	SI	La direcció revisarà les polítiques un cop l'any.
6. Aspectes Organitzatius de la seguretat de la informació					
	6.1. Organització Interna.				
		6.1.1. Assignació de responsabilitats per a la seguretat de la informació.	L2	SI	Existeixen uns rols definits amb les seves responsabilitats aprovats per la direcció.
		6.1.2. Segregació de taques.	L3	SI	Les tasques venen definides pels diferents rols.
		6.1.3. Contacte amb les autoritats.	L3	SI	Existeixen diferents documents i polítiques al respecte.
		6.1.4. Contacte amb els grups d'interès especial.	L2	SI	Existeix una política de compliment per al contacte amb grups de seguretat.
		6.1.5. Seguretat de la informació a la gestió de projectes.	L5	SI	Existeix una política per a la gestió de projectes i els seus canvis.
	6.2. Dispositius per a la mobilitat i el teletreball.				
		6.2.1. Política d'ús	L5	SI	Existeixen

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
		de dispositius per a la mobilitat.			polítiques per a l'ús de dispositius mòbils i manipulació de medis mòbils. S'ha instal·lat un MDM.
		6.2.2. Teletreball.	L4	SI	Es comproven amb periodicitat els usuaris que accedeixen al teletreball.
7. Seguretat lligada als recursos humans.					
	7.1. Abans de la contractació.				
		7.1.1. Investigació d'antecedents.	L2	SI	El departament de RRHH té polítiques assignades al respecte.
		7.1.2. Termes i condicions de contractació.	L5	SI	S'informa als nous empleats de les normes de seguretat de la companyia per part de RRHH.
	7.2. Durant la contractació.				
		7.2.1. Responsabilitats de gestió.	L4	SI	La política de seguretat és pública per al personal i tercers.
		7.2.2. Conscienciació, educació i capacitació en seguretat de la informació.	L5	SI	S'ha aplicat un projecte de formació en seguretat de la informació per als empleats.
		7.2.3. Procés disciplinari.	L4	SI	La política de seguretat de RRHH contempla les normes de obligatori compliment per els usuaris.
	7.3. Cessament o canvi de lloc de treball.				
		7.3.1. Cessament o canvi de lloc de treball.	L2	NO	Encara que està documentat, no s'aconsegueix una comunicació fluida entre departaments.
8. Gestió d'actius.					
	8.1. Responsabilitat sobre els actius.				
		8.1.1. Inventari	L4	SI	Existeix una

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
		d'actius.			política i una aplicació pròpia on es troben tots els actius registrats.
		8.1.2. Propietat dels actius.	L4	NO	Existeixen actius sense assignar.
		8.1.3. Ús acceptable dels actius.	L4	SI	S'ha generat una política amb el procediment de l'ús de la informació.
		8.1.4. Devolució d'actius.	L3	SI	La devolució dels actius es realitza sota el control del departament de RRHH i Sistemes de la informació. Un cop retornat l'actiu es modifica l'inventari.
	8.2. Classificació de la informació.				
		8.2.1. Directrius de classificació.	L5	SI	La informació de la companyia es troba classifica un cop aplicat el projecte proposat.
		8.2.2. Etiquetatge i manipulació de la informació.	L5	SI	La informació de la companyia es troba classifica un cop aplicat el projecte proposat.
		8.2.3. Manipulació d'actius.	L4	SI	S'han establert polítiques que indiquen el procediment de manipulació dels actius.
	8.3. Maneig dels suports d'emmagatzematge				
		8.3.1. Gestió de suports extraïbles.	L4	SI	S'ha solucionat el problema de control dels dispositius USB mitjançant polítiques establertes al MDM de la companyia.
		8.3.2. Eliminació de suports.	L4	SI	S'ha generat un procediment per a la correcta eliminació dels suports un cop retirats.
		8.3.3. Suports	L4	SI	S'ha instal·lat un

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
		físics en transit.			MDM que controla i xifra la documentació en transit.
9. Control d'accés.					
	9.1. Requisits de negoci per al control d'accessos.				
		9.1.1. Política de control d'accessos.	L4	SI	S'ha documentat la política de control d'accés.
		9.1.2. Control d'accés a les xarxes i serveis associats.	L4	SI	Els usuaris tenen accés a les utilitats i serveis assignats pels seus responsables..
	9.2. Gestió d'accés d'usuari.				
		9.2.1. Gestió d'altes/baixes al registre d'usuaris.	L5	SI	Existeix una utilitat pròpia enllaçada amb la utilitat d'incidències per sol·licitar tant les altes com les baixes d'usuaris des de RRHH al departament d'infraestructura de la informació.
		9.2.2. Gestió dels drets d'accés assignats a usuaris.	L4	SI	S'ha documentat el procediment d'assignació de permisos d'usuaris.
		9.2.3. Gestió dels drets d'accés amb privilegis especials.	L2	NO	Aquests tipus d'accessos es sol·liciten mitjançant incidència des de el responsable del departament afectat.
		9.2.4. Gestió d'informació confidencial d'autenticació d'usuaris.	L4	SI	Tota la informació confidencial que tingui l'usuari per a la seva autenticació vindrà donada per la utilitat d'altes i baixes al personal indicat.
		9.2.5. Revisió dels drets d'accés dels usuaris.	L4	SI	S'ha documentat i s'ha establert una revisió dels accessos dels usuaris.
		9.2.6. Retirada o adaptació dels drets d'accés.	L4	SI	Es realitzen les baixes d'usuari a petició del

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
					departament de RRHH cap al departament d'infraestructura de la informació mitjançant la utilitat pròpia d'altes i baixes.
	9.3. Responsabilitats de l'usuari.				
		9.3.1. Ús d'informació confidencial per a l'autenticació.	L5	SI	S'ha documentat i notificat la política i el procediment d'ús de la informació confidencial.
	9.4. Control d'accés a sistemes i aplicacions.				
		9.4.1. Restricció de l'accés a la informació	L3	NO	L'accés a les dades es troba restringit en funció del nivell o necessitat de cada usuari. Però no es troba documentat.
		9.4.2. Procediments segurs d'inici de sessió.	L3	SI	Totes les aplicacions i dades de la companyia requereixen d'un inici de sessió amb usuari i contrasenya. Existeix una política de contrasenyes.
		9.4.3. Gestió de contrasenyes d'usuari.	L4	SI	Existeix una política de contrasenyes implantada on es troba indicat la caducitat de la contrasenya, l'històric i el nivell de seguretat mínim de la mateixa.
		9.4.4. Ús d'eines d'administració de sistemes.	L4	SI	S'han modificat les polítiques de software no acceptat per la companyia adaptat a la situació i negoci actual.
		9.4.5. Control d'accés al codi font dels programes.	L4	SI	S'han documentat i assegurat els accessos al codi font per part del departament de

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
					sistemes.
10. Xifratge					
	10.1. Controls criptogràfic.				
		10.1.1. Política d'ús dels controls criptogràfics.	L3	SI	S'ha establert una política per a l'ús dels controls criptogràfics.
		10.1.2. Gestió de claus.	L0	NO	No existeix cap tipus de gestió de les claus criptogràfiques.
11. Seguretat física i ambiental.					
	11.1. Àrees segures.				
		11.1.1. Perímetre de seguretat física.	L4	SI	Existeix un control d'accessos informatitzat i control físics a l'entrada de l'edifici.
		11.1.2. Controls físics d'entrada.	L4	SI	Existeix un control d'accés a l'entrada de l'edifici i del complex d'oficines.
		11.1.3. Seguretat d'oficines, despatxos i recursos.	L4	SI	Els diferents accessos es realitzen mitjançant clau, menys al CPD on existeix un lector d'empremta connectat al software de control d'accés.
		11.1.4. Protecció contra amenaces externes i ambientals.	L4	SI	La companyia disposa d'un generador elèctric en una part elevada per no tindre problemes de funcionament en cas d'inundació i poder garantir el subministrament elèctric del CPD, també es disposa d'un sistema d'extinció d'incendis.
		11.1.5. El treball en àrees segures.	L4	SI	En el cas de treballs al CDP, és disposa d'un procediment de treball ja que la sala disposa d'un sistema

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
					d'extinció d'incendis.
		11.1.6. Àrees d'accés públic, càrrega i descàrrega.	No aplica	-	-
	11.2. Seguretat dels equips.				
		11.2.1. Emplaçament i protecció d'equips.	L3	SI	Els equips es troben ubicats en llocs adequats a la realització de les seves tasques.
		11.2.2. Instal·lacions de subministre.	L4	SI	Els equips del CPD es tenen unitats SAI i un generador per garantir el subministrament elèctric.
		11.2.3. Seguretat del cablejat.	L4	SI	El cablejat es troba controlat, aïllat i amb tota la instal·lació documentada i certificada.
		11.2.4. Manteniment dels equips.	L4	SI	Els equips es troben en constant manteniment de les seves aplicacions i necessitats. Tenim documentat el procediment d'actualitzacions d'antivirus i software Microsoft.
		11.2.5. Sortida d'actius fora de les dependencies de l'empresa.	L4	SI	Es registren totes les peticions de sortida d'actius mitjançant incidència.
		11.2.6. Seguretat dels equips i actius fora de les instal·lacions.	L4	SI	Els actius que surten temporalment de les instal·lacions es troben afectats per les polítiques definides al MDM.
		11.2.7. Reutilització o retirada segura de dispositius d'emmagatzematge.	L4	SI	S'ha documentat el procediment de reutilització o retirada d'equips per part del departament d'infraestructures de la informació.
		11.2.8. Equip	L4	SI	S'ha format als

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
		informàtic d'usuari desatès.			usuaris en temes de seguretat de la informació i a la política de seguretat s'indica aquest procediment.
		11.2.9. Política de lloc de treball aclarit i bloqueig de pantalla.	L4	SI	S'ha format als usuaris en temes de seguretat de la informació i a la política de seguretat s'indica aquest procediment.
12. Seguretat en la operativa.					
	12.1. Responsabilitats i procediments d'operació.				
		12.1.1. Documentació de procediments d'operació.	L4	SI	S'han documentat tots els procediments.
		12.1.2. Gestió de canvis.	L4	SI	El departament de sistemes d'informació ha documentat tots els procediments de seguretat.
		12.1.3. Gestió de capacitats.	L3	SI	Es realitza una previsió anual per part del departament d'infraestructura de la informació.
		12.1.4. Separació d'entorns de desenvolupament, prova i producció.	L2	SI	Els entorns de desenvolupament es troben en xarxes aïllades de la de producció de la companyia.
	12.2. Protecció contra codi maliciós.				
		12.2.1. Controls contra codi maliciós	L4	SI	Existeix un software antivirus que s'actualitza des d'una ubicació interna a tots els equips de la xarxa i s'informa a tots els usuaris de noves amenaces mitjançant noticies a l'Intranet corporativa.
	12.3. Còpies de seguretat.				

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
		12.3.1. Còpies de seguretat de la informació.	L5	SI	Existeixen polítiques de copia de seguretat per a tots els sistemes centrals, es realitzen proves de recuperació periòdiques establertes al projecte implantat.
	12.4. Registre d'activitat i supervisió.				
		12.4.1. Registre i gestió d'esdeveniments d'activitat.	L3	SI	Queden enregistrats el inicis de sessió dels usuaris en els logs dels servidors.
		12.4.2. Protecció dels registres d'informació.	L1	NO	No es realitza cap tipus de backup dels logs d'accés d'usuaris. Encara que no són accessibles públicament.
		12.4.3. Registres d'activitat de l'administrador i operador del sistema.	L0	NO	No queden registrades les operacions dels administradors.
		12.4.4. Sincronització de rellotges.	L5	SI	Tota la xarxa sincronitza els seus rellotges a nivell de domini, existint un servidor d'hora intern encarregat de la sincronització.
	12.5. Control del software d'explotació				
		12.5.1. Instal·lació del software a sistemes de producció.	L4	SI	Totes les actualitzacions dels sistemes operatius venen controlades per l'administrador mitjançant polítiques del domini.
	12.6. Gestió de la vulnerabilitat tècnica.				
		12.6.1. Gestió de les vulnerabilitats tècniques.	L3	SI	Es controla per part del departament d'infraestructura de la informació les noves vulnerabilitats

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
					existents.
		12.6.2. Restriccions a la instal·lació de software.	L5	SI	S'ha generat una política per a la instal·lació de software.
	12.7. Consideracions de les auditories dels sistemes d'informació.				
		12.7.1. Controls d'auditoria dels sistemes d'informació.	L3	SI	Existeixen auditories externes periòdiques.
13. Seguretat a les telecomunicacions.					
	13.1. Gestió de la seguretat a les xarxes.				
		13.1.1. Controls de xarxa.	L4	SI	S'ha generat una política per a la seguretat de la xarxa.
		13.1.2. Mecanismes de seguretat associats a serveis de xarxa.	No aplica	-	-
		13.1.3. Segregació de xarxes.	L5	SI	Tota la xarxa es troba segregada en funció del tipus d'equip que es connecta. La documentació es troba a disposició del departament d'infraestructura de la informació.
	13.2. Intercanvi d'informació amb parts externes.				
		13.2.1. Polítiques i procediments d'intercanvi d'informació.	L5	SI	Existeix un procediment de recuperació de sistema en cas de caiguda per poder continuar amb el servei d'intercanvi. Aquest servei es troba gestionat per un tercers i allotjat a les nostres oficines (no centrals). Han millorat les comunicacions entre seus.
		13.2.2. Acords d'intercanvi.	L4	SI	Existeixen transferències d'informació amb tercers per part del departament

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
					de RRHH fent servir aplicacions especifiques aportades pel proveïdor.
		13.2.3. Missatgeria electrònica.	L4	SI	Existeixen mecanismes de filtratge de correu electrònic (filtre AntiSpam) administrats pel departament d'infraestructura de la informació, a l'hora d'una rèplica de servei fora de les instal·lacions centrals.
		13.2.4. Acords de confidencialitat i secret.	L3	SI	El departament de RRHH juntament amb el jurídic aporta els documents a signar per els treballadors susceptibles a treballar amb documentació sensible.
14. Adquisició, desenvolupament i manteniment dels sistemes d'informació.					
	14.1. Requisits de seguretat dels sistemes d'informació.				
		14.1.1. Anàlisi i especificació dels requisits de seguretat.	L4	SI	S'ha documentat i generat una política per controlar els requisits de seguretat del sistemes.
		14.1.2. Seguretat de les comunicacions en serveis accessibles per xarxes públiques.	L3	SI	Tota informació accessible des de les xarxes públiques passa per un firewall i requereixen de validació mitjançant usuari i contrasenya. Existeix una política de segureta en xarxa.
		14.1.3. Protecció de les transaccions per xarxes telemàtiques.	L4	SI	Tota informació accessible des de les xarxes públiques passa per un firewall i requereixen de

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
					validació mitjançant usuari i contrasenya. Es disposa de logs per comprovar les connexions. Existeix una política de seguretat en xarxa.
	14.2. Seguretat als processos de desenvolupament i suport.				
		14.2.1. Política de desenvolupament segur de software.	L3	SI	El departament de sistemes disposa de polítiques per al desenvolupament de software.
		14.2.2. Procediments de control de canvis als sistemes.	L2	NO	Es valora la viabilitat del canvi per part dels responsables del departament de tecnologies de la informació. Encara que no hi ha cap política que ho controli.
		14.2.3. Revisió tècnica de les aplicacions després d'efectuar canvis al sistema operatiu.	L2	SI	El departament d'infraestructura de la informació s'encarrega de controlar la compatibilitat de les aplicacions amb els nous sistemes operatius.
		14.2.4. Restriccions als canvis en els paquets de software.	L2	SI	Tots els canvis realitzats sobre paquets d'instal·lació de software de tercers es generaran pel departament d'infraestructura de la informació de forma controlada.
		14.2.5. Ús de principis d'enginyeria en protecció de sistemes.	L2	SI	El departament d'infraestructura de la informació genera i manté la informació necessària dels sistemes de la companyia.
		14.2.6. Seguretat en entorns de desenvolupament.	L1	NO	Els entorns de desenvolupament no tenen totes les mesures de

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
					seguretat desitjables.
		14.2.7. Externalització del desenvolupament de software.	L5	SI	El departament d'infraestructura de la informació es troba en constant comunicació amb els proveïdors de desenvolupament o adaptació de software.
		14.2.8. Proves de funcionalitat durant el desenvolupament dels sistemes.	L4	SI	Es realitzen diferents proves de funcionalitat per membres del departament de tecnologies de la informació.
		14.2.9. Proves d'acceptació.	L3	SI	Es realitzen enquestes als usuaris per valorar la viabilitat d'implantació de noves versions.
	14.3. Dades de prova.				
		14.3.1. Protecció de les dades utilitzades en proves.	L5	SI	Les dades utilitzades per a les proves no són dades de producció, si no BBDD específiques per aquests processos.
15. Relacions amb subministradors.					
	15.1. Seguretat de la informació a les relacions amb subministradors.				
		15.1.1. Política de seguretat de la informació per a subministradors.	L4	SI	La companyia disposa de polítiques i procediments per a controlar l'accés de tercers als seus sistemes.
		15.1.2. Tractament del risc dintre dels acords de subministradors.	L4	SI	La companyia disposa de contractes amb cadascun dels subministradors, S'ha establert una política de seguretat per als proveïdors.
		15.1.3. Cadena de subministrament en tecnologies de la informació i	L2	NO	La companyia no disposa de tots els acords amb els proveïdors

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
		comunicacions.			existents a la cadena de subministrament dels serveis.
	15.2. Gestió de la prestació del servei per subministradors.				
		15.2.1. Supervisió i revisió del serveis prestats per tercers.	L3	SI	Existeix una política per auditar el servei dels proveïdors.
		15.2.2. Gestió de canvis als serveis prestats per tercers.	L3	SI	El departament afectat pels canvis del proveïdor, valora la continuïtat del servei basant-se en la política de la companyia.
16. Gestió d'incidents a la seguretat de la informació.					
	16.1. Gestió d'incidents de seguretat de la informació i millores.				
		16.1.1. Responsabilitats i procediments.	L4	SI	Es troben documentats els rols i responsabilitats.
		16.1.2. Notificació dels esdeveniments de seguretat de la informació.	L4	SI	La companyia disposa d'una utilitat de ticketing per a gestionar tots els incidents.
		16.1.3. Notificació de punts dèbils de la seguretat.	L4	SI	Es fa servir la mateixa utilitat que en el punt anterior.
		16.1.4. Valoració d'esdeveniments de seguretat de la informació i presa de decisions.	L3	SI	El departament d'infraestructures de la informació revisa i controla els esdeveniments de seguretat.
		16.1.5. Resposta als incidents de seguretat.	L4	SI	Tots els procediments de seguretat es troben documentats.
		16.1.6. Aprenentatge dels incidents de seguretat de la informació.	L2	NO	La companyia no disposa de cap base de coneixement on enregistrar solucions a incidents ocorreguts.
		16.1.7. Recopilació	L1	NO	Només es

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
		d'evidències.			recopilen dades en cas de problema de seguretat.
17. Aspectes de seguretat de la informació a la gestió de la continuïtat del negoci.					
	17.1. Continuïtat de la seguretat de la informació.				
		17.1.1. Planificació de la continuïtat de la seguretat de la informació.	L4	SI	Existeix un protocol de recuperació dels sistemes crítics.
		17.1.2. Implantació de la continuïtat de la seguretat de la informació.	L4	SI	Existeix una política per a la continuïtat del negoci.
		17.1.3. Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	L4	SI	Es revisen els controls 17.1.1 segons indica la política de continuïtat del negoci.
	17.2. Redundàncies.				
		17.2.1. Disponibilitat d'instal·lacions per al processament de la informació.	L5	SI	Existeixen sistemes replicats a una seu remota per a solvatar possibles problemes de seguretat al CPD central.
18. Compliment.					
	18.1. Compliment dels requisits legals i contractuals.				
		18.1.1. Identificació de la legislació aplicable.	L3	SI	Es disposa de documents on es registra la documentació legal que aplica a la companyia.
		18.1.2. Drets de propietat intel·lectual (DPI).	L4	SI	La companyia disposa d'una auditoria de software recent.
		18.1.3. Protecció dels registres de l'organització.	L4	SI	Existeix un procediment de copia d'informació.
		18.1.4. Protecció de dades i privacitat de la informació personal.	L3	SI	Les dades personals dels treballadors no són accessibles per la resta d'usuaris, només per usuaris amb

Dominis	Objectius de control	Controls	CMM	Compli-ment	Observacions
					permisos d'accés especials.
		18.1.5. Regulació dels controls criptogràfics.	L3	SI	La companyia disposa d'usuaris amb signatura electrònica per a determinats processos.
	18.2. Revisions de la seguretat de la informació.				
		18.2.1. Revisió independent de la seguretat de la informació.	L4	SI	La companyia està sotmesa a auditories independents de forma periòdica.
		18.2.2. Compliment de les polítiques i normes de seguretat.	L4	SI	Existeix una política de compliment on s'estableix la periodicitat de revisió per la direcció.
		18.2.3. Comprovació del compliment.	L4	SI	Existeixen polítiques on s'indica la periodicitat de revisió i les normes de seguretat del sistemes.