Pla Director de Seguretat de la Informació de Traun

Nom Estudiant: Maria Montserrat Ponce León

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

Consultor: Arsenio Tortajada Gallego

Data Lliurament: 06/06/2016

- **Introducció**
- Fase 1: Situació actual
- Fase 2: Sistema de Gestió Documental
- Fase 3: Anàlisis de Riscos
- Fase 4: Propostes de Projectes
- Fase 5: Auditoria de Compliment
- Conclusions

INTRODUCCIÓ

- PLA DE SEGURETAT
  - Per què el fem?

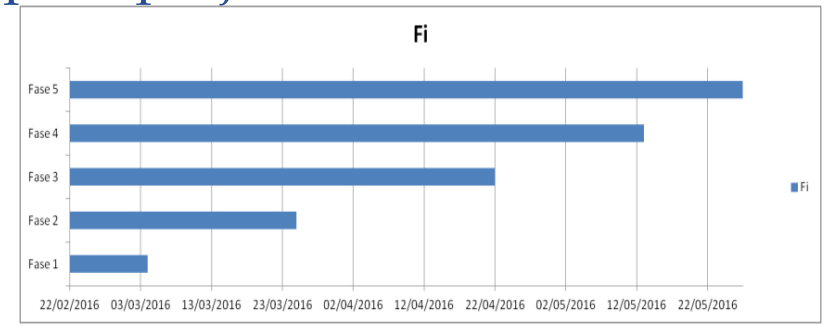
Les organitzacions consideren la informació com un dels seus valors més importants.

  - Què ens aporta?

Precisar l'estat de la seguretat de la informació actual en relació als diferents aspectes de la ISO/IEC 27001.

  - Com el realitzem?

La realització d'aquest projecte s'ha dividit en cinc fases:

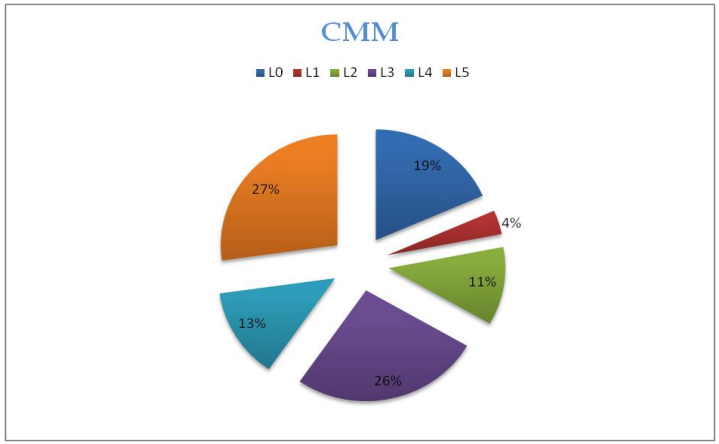


- Introducció
- **Fase 1: Situació actual**
- Fase 2: Sistema de Gestió Documental
- Fase 3: Anàlisis de Riscos
- Fase 4: Propostes de Projectes
- Fase 5: Auditoria de Compliment
- Conclusions

Fase 1: Situació actual

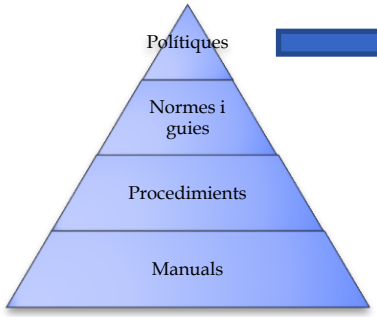
114 controls o mesures preventives , organitzats en 14 àrees i 35 objectius de control de la i ISO/IEC 27002

Controls	Situació Actual
5. Polítiques de la Seguretat de la Informació	L5
6. Organització de la Seguretat de la Informació	L3
7. La Seguretat dels recursos humans	L2
8. Gestió d'actius	L2
9. Control d'accés	L3
10 Criptografia	L0
11 La seguretat física i ambiental	L3
12 Operacions de Seguretat	L5
13 Seguretat de les comunicacions	L4
14 Sistema d'adquisició, desenvolupament i manteniment	L3
15 Les relacions amb proveïdors	L4
16 Gestió d'incidents de seguretat d'informació	L0
17 Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	L5
18 Compliment	L5



- Introducció
- Fase 1: Situació actual
- **Fase 2: Sistema de Gestió Documental**
- Fase 3: Anàlisis de Riscos
- Fase 4: Propostes de Projectes
- Fase 5: Auditoria de Compliment
- Conclusions

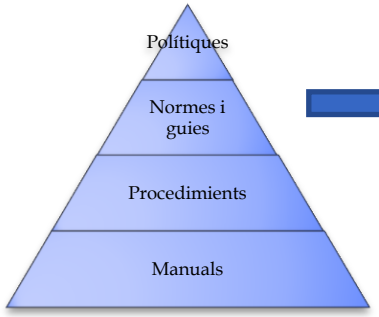
Fase 2: Sistema de Gestió Documental



Política de Seguretat

- L'ús dels sistemes informàtics.
- La identificació i control d'accés al sistema.
- La confidencialitat de la informació.
- L'ús de serveis.
- Incidències i infraccions de seguretat de la informació.

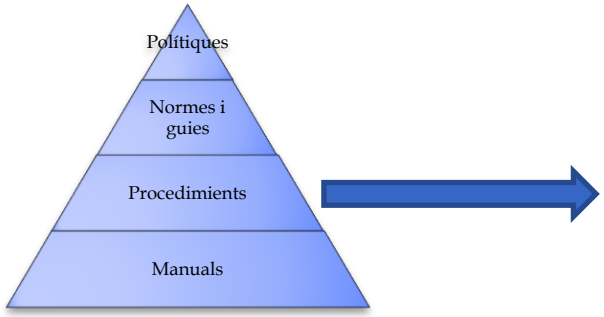
Fase 2: Sistema de Gestió Documental



Gestió de Rols i Responsabilitats
Gestió d'Indicadors
Declaració d'Aplicabilitat

- Estructura Organitzativa sobre la seguretat
- Determinar l'eficacia de les mesures de seguretat implementades
- Controls a implementar en el SGSI

Fase 2: Sistema de Gestió Documental



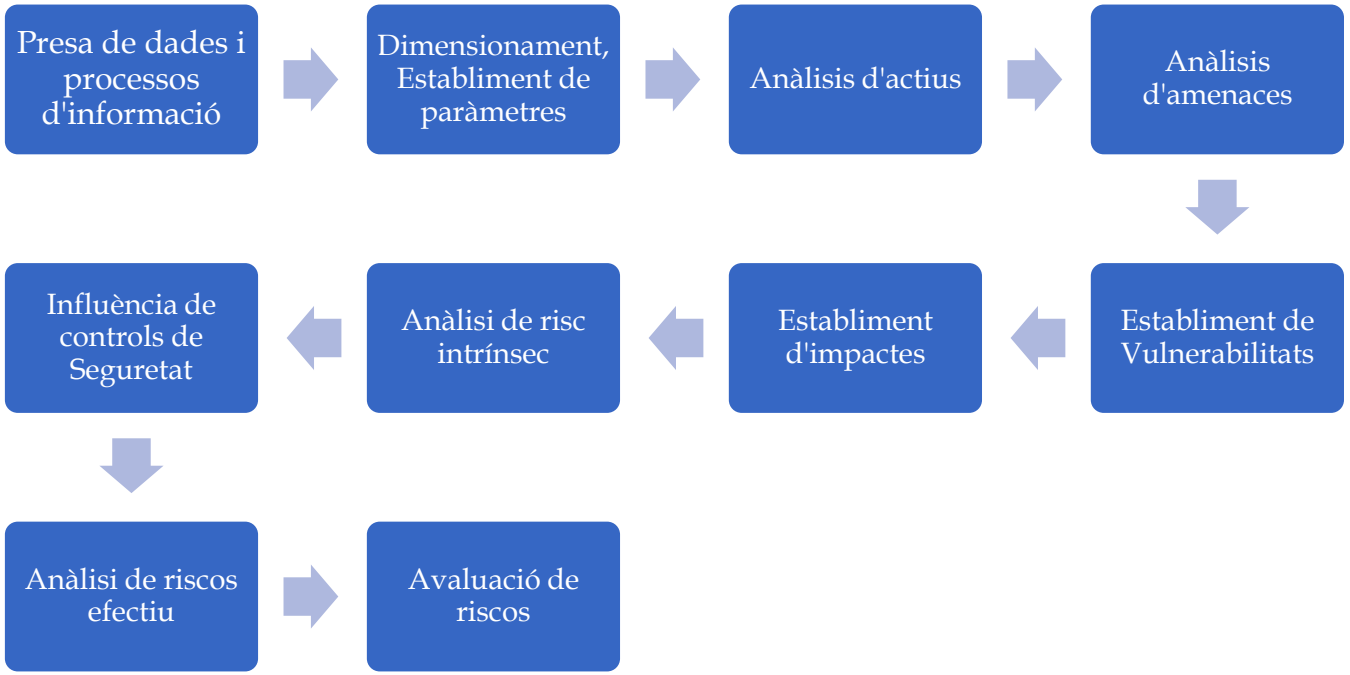
Procediment d'Auditories Internes
Procediment de Revisió per Direcció
Metodologia de Anàlisis de Riscos

- Estructura Organitzativa sobre la seguretat
- Determinar l'eficacia de les mesures de seguretat implementades
- Controls a implementar en el SGSI

- Introducció
- Fase 1: Situació actual
- Fase 2: Sistema de Gestió Documental
- **Fase 3: Anàlisis de Riscos**
- Fase 4: Propostes de Projectes
- Fase 5: Auditoria de Compliment
- Conclusions

Fase 3: Anàlisis de Riscos

- La metodologia utilitzada MAGERIT v.3
- Magerit segueix les fases següents:



Fase 3: Anàlisis de Riscos

Presa de dades i processos d'informació

- Reducció dels actius, no s'inclouen la part de fàbrica, únicament IT.

Dimensionament, Establiment de paràmetres

- Els paràmetres que s'han d'identificat són els següents:
  - Valor dels actius.
  - Vulnerabilitat.
  - Impacte.
  - Efectivitat del control de seguretat

Fase 3: Anàlisis de Riscos

Valor dels actius

Valoració d'actius		
Descripció	**Abreviatura**	**Valor**
Molt alt	MA	300.000
Alt	A	150.000
Mitjà	M	75.000
Baix	B	30.000
Molt baix	MB	10.000
Menyspreable	D	5.000

Efectivitat del control de seguretat

Impacte/Vulnerabilitat		
Descripció	Abreviatura	Valor
Molt Alt	MA	95%
Alt	A	75%
Mitjà	M	50%
Baix	B	30%
Molt Baix	MB	10%

Vulnerabilitat

Freqüència			
Descripció	**Rang**	**Abreviatura**	**Valor**
Extremadament freqüent	1 vegada al dia	EF	1
Molt freqüent	1 vegada cada dos setmanes	MF	0,071232877
Freqüent	1 vegada cada dos mesos	F	0,016438356
Poc Freqüent	1 vegada cada quatre mesos	PF	0,010958904
Molt poc freqüent	1 vegada cada 6 mesos	MPF	0,005479452
Menyspreable	1 vegada a l'any	D	0,002739726

Impacte

Impacte		
Descripció	Abreviatura	Valor
Crític	C	90%
Alt	A	75%
Mitjà	M	50%
Baix	B	20%

Fase 3: Anàlisis de Riscos

Anàlisis d'actius → Anàlisis d'amenaces

Àmbit	Codi	Quantita	Actiu	alor Qualitati	alor Quantitati	otal valor Quantitati
Instal·la	I.4	50	Llocs de treball dividó d'operació	M	75000	3750000
	I.5	15	Llocs de treball divisó industrial	A	150000	2250000
	I.6	10	Llocs de treball comercial	B	30000	300000
	I.7	38	Sales d'impressió	MB	10000	380000
Hardware	HW.1	12	Firewalls	A	150000	1800000
	HW.2	5	Proxys	M	75000	375000
	HW.3	6	Siem	M	75000	450000
	HW.4	3	IPS	M	75000	225000
	HW.5	4	Qualys	M	75000	300000
	HW.6	15	Load Balancer	M	75000	1125000
	HW.7	150	Routers	M	75000	11250000
	HW.8	115	Impresores	MB	10000	1150000
	HW.9	600	Workstations	M	75000	45000000
	HW.10	2500	Laptops	M	75000	187500000
	HW.11	1000	Mòbils	MB	10000	10000000
	HW.12	50	AIX 6	MA	300000	15000000
	HW.13	8	Cabina de discos SATA – Dades	MA	300000	2400000
	HW.14	102	VMWARE ESXi	MA	300000	30600000
	HW.15	2	Backups	A	150000	300000
	HW.16	6	Commutadors xarxa	A	150000	900000
Aplicació i software	SW.1	200	SCADA	MA	300000	60000000
	SW.2	3900	Windows 7	M	75000	292500000
	SW.3	136	Windows Server 2003	MB	10000	1360000
	SW.4	530	Windows server 2008 R2	MA	300000	159000000
	SW.5	95	Windows server 2012 R2	MA	300000	28500000
	SW.6	18	Red Hat Enterprise Linux 5.9	M	75000	1350000
	SW.7	116	Red Hat Enterprise Linux 6.5	A	150000	17400000
	SW.8	36	Red Hat Enterprise Linux 6.7	MA	300000	10800000
	SW.9	148	Apache Tomcat	A	150000	22200000
	SW.10	29	IIS	A	150000	4350000
	SW.11	78	SQL	A	150000	11700000
	SW.12	45	Oracle 10g	M	75000	3375000
	SW.13	92	Oracle 11g	A	150000	13800000
	SW.14	37	Oracle 12c	MA	300000	11100000
	SW.15	63	Solaris 11	M	75000	4725000
	SW.16	2	AD RHH	M	75000	150000
	SW.17	26	SAP	A	150000	3900000
	SW.18	1	Antivirus	M	75000	75000

Paràmetres | Actius | Valoració actiu | Gràfiques valoració Actius | Dimensiona

Tipus	Codi	Amenaça	Actiu Afectat						
			I	HW	SW	D	X	S	EA	P
Amenaces d'origen natural	AM-01	Incendi	X	X					X	
	AM-02	Inundació	X	X					X	
	AM-03	Desastre natural	X	X					X	
	AM-04	Atac físic	X	X					X	
	AM-05	Fallada / avaria d'equip	X	X					X	
	AM-06	Avaria climatització	X	X					X	
	AM-07	Errades subministrament elèctric	X	X					X	
nenaces d'entorn o d'origen industr	AM-08	Robatori personal intern		X	X					
	AM-09	Manipulació d'equipamient		X	X					
	AM-10	indisponibilitat física	X	X			X		X	X
	AM-11	indisponibilitat lògica			X	X				
	AM-12	indisponibilitat personal								X
	AM-13	Indisponibilitat de comunicacions					X			
Errors i errors no intencionats	AM-14	Error de disseny			X	X				
	AM-15	Manca de manteniment programari			X	X	X			
	AM-16	Errors humans	X	X	X	X	X	X	X	X
	AM-17	Pèrdua d'informació				X				
	AM-18	Pèrdua de documents				X				X
	AM-19	Fallades de programari			X	X				
	AM-20	Fallada en còpies		X	X	X				
	AM-21	Fallada en les comunicacions					X			
Atacs intencionats	AM-22	Eliminacion no autoritzada				X				X
	AM-23	Robatori persones externes			X	X				X
	AM-24	Atac informàtic		X	X	X	X	X		
	AM-25	Coacció				X				X
	AM-26	Negligència	X	X	X	X	X			X

Paràmetres | Actius | Valoració actiu | Gràfiques valoració Actius | Dimensionar

Fase 3: Anàlisis de Riscos

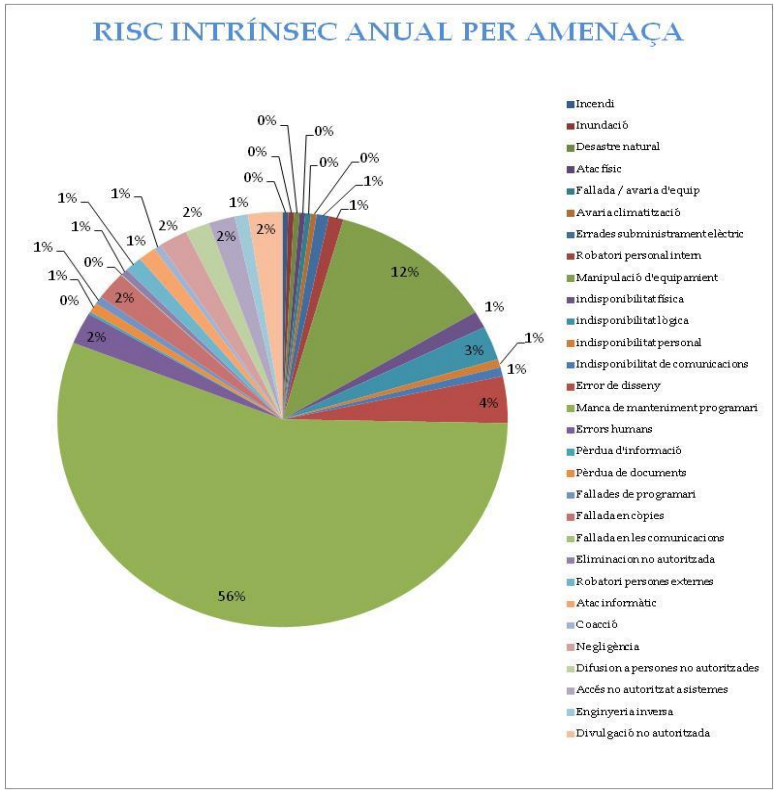
Establiment de Vulnerabilitats → Establiment d'impactes

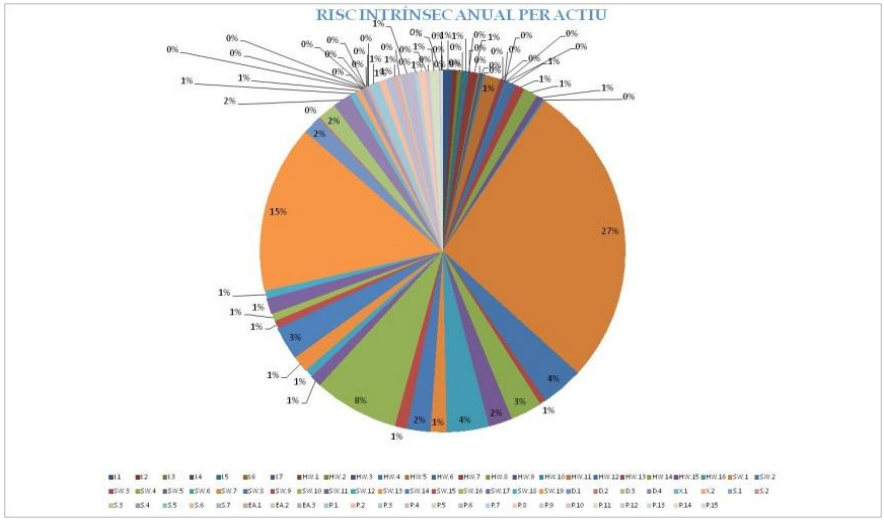
	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC	BD	BE	BF
	indisponibilitat lògica	indisponibilitat personal		Indisponibilitat de comunic		Error de disseny		Manca de manteniment proc		Errors humans		Pèrdua d'informació		Pèrdua de documents		Fallades de programari		Fallada en còpies		Fallada en les comunicacions		Eliminacion no autoritzada		Robatori persones externes		Atac informàtic		Coacció		Negligència		Difusion a persones no autor		Accés no autoritzat a sistema	
Codi	AM-11	AM-12		AM-13		AM-14		AM-15		AM-16		AM-17		AM-18		AM-19		AM-20		AM-21		AM-22		AM-23		AM-24		AM-25		AM-26		AM-27		AM-28	
I.1	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0
I.2	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0
I.3	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	MPF	0,005479	-	0	-	0
I.4	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0
I.5	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0
I.6	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0
I.7	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0
HW.1	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	F	0,016438	-	0	MPF	0,005479	-	0	-	0
HW.2	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	F	0,016438	-	0	F	0,016438	-	0	-	0
HW.3	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0
HW.4	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0
HW.5	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	EF	1,000000	-	0	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0
HW.6	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0
HW.7	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	F	0,016438	-	0	F	0,016438	-	0	-	0
HW.8	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	F	0,016438	-	0	-	0
HW.9	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	F	0,016438	-	0	-	0
HW.10	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	F	0,016438	-	0	-	0
HW.11	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	F	0,016438	-	0	-	0
HW.12	0	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0

Paràmetres | Actius | Valoració actiu | Gràfiques valoració Actius | Dimensionament | Amenaces | **Freqüència** | Impacte Potencial | Risc Intrínsec i Freqüència | Gràfiques Risc Intrín

Fase 3: Anàlisis de Riscos

Anàlisi de risc intrínsec

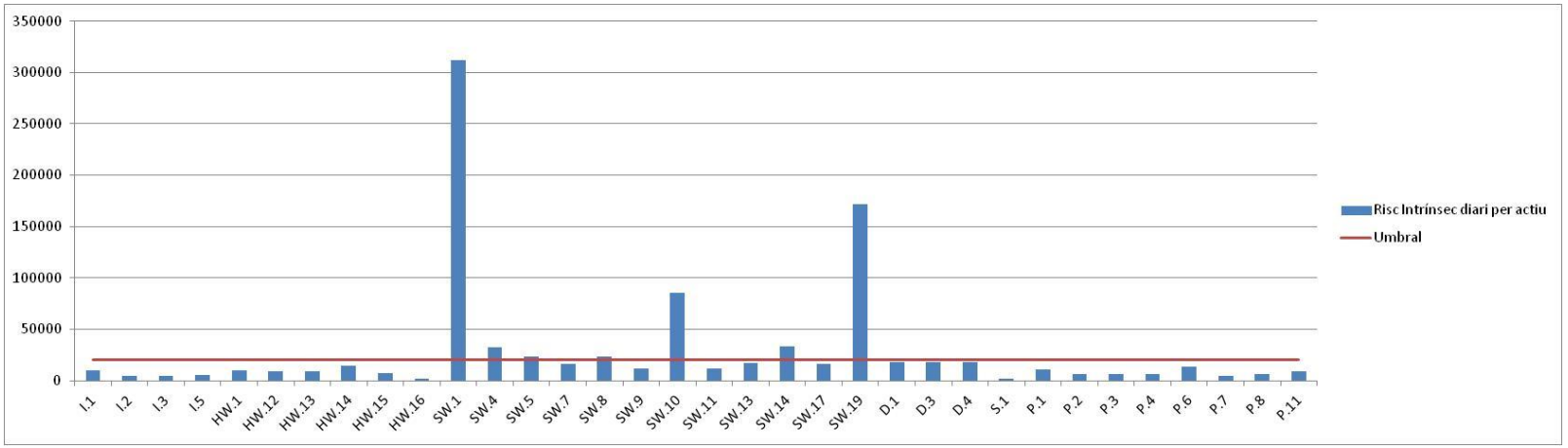




Risc Intrínsec = Impacte Potencial x Freqüència

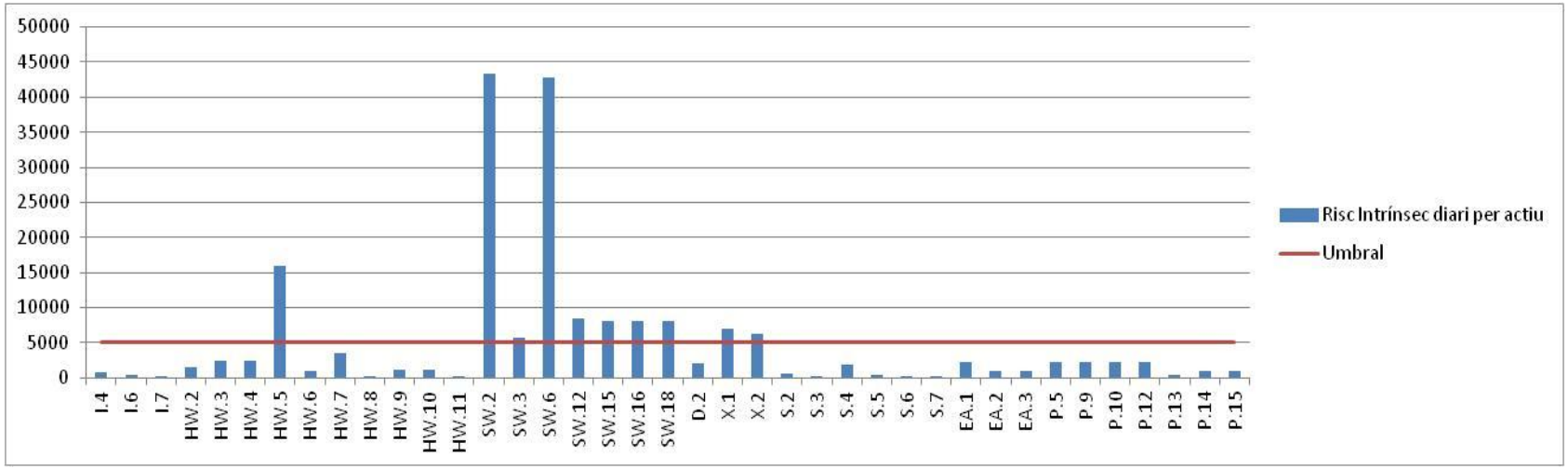
Fase 3: Anàlisis de Riscos

Llindar 20.000 euros



Fase 3: Anàlisis de Riscos

Llindar 5.000 euros



Fase 3: Anàlisis de Riscos

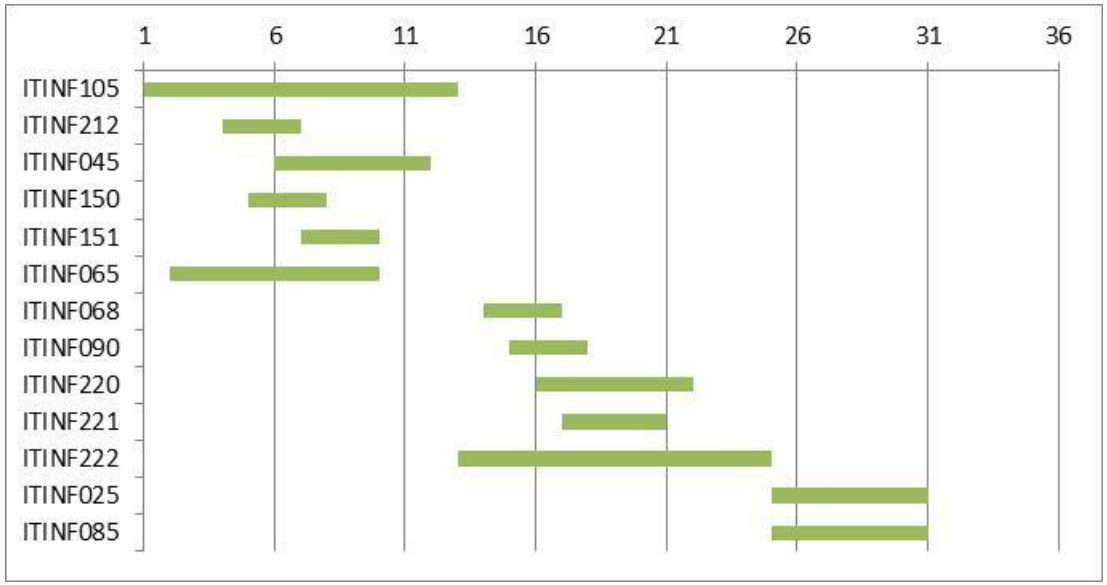
En tots els anàlisi podem observar que els principals problemes de l'organització són:

- La manca de manteniment de programari.
- Centralitzar tot els software, hardware, etc en IT.
- Millorar l'antivirus, seus distribuïdes mundialment son un gran focus d'infecció.
- Actualització de sofware (Windows, Oracle, etc).
- Falta d'implementació d'un procediment de backups amb un software actual.
- Millorar les instal·lacions del principal CPD d'Espanya.
- Millora del procés de pegats i auditories de compliment normatiu, Qualys.

- Introducció
- Fase 1: Situació actual
- Fase 2: Sistema de Gestió Documental
- Fase 3: Anàlisis de Riscos
- **Fase 4: Propostes de Projectes**
- Fase 5: Auditoria de Compliment
- Conclusions

Fase 4: Propostes de Projectes

- Projectes a curt termini: realització e implantació durant el primer any.
- Projectes a mig termini: realització e implantació durant el segon any.
- Projectes a llarg termini: realització e implantació durant el tercer any.



Fase 4: Propostes de Projectes

- Projectes a curt termini:

- ITINF105:Realització de l'inventari d'actius (CMDB).
- ITINF212: Implementació advanced threat detection.
- ITINF045: Programa de conscienciació sobre la seguretat.
- ITINF150: Implementació de pegats Red Hat.
- ITINF151: Actualització del sofware de backups.
- ITINF065: Millora dels Centre de Processament de Dades

Fase 4: Propostes de Projectes

- Projectes a mig termini:

  - ITINF068: Implementació Policy Compliance, auditories de compliment normatiu.
  - ITINF090: Procés de gestió de backups
  - ITINF220: Migració Windows 2003 a Windows server 2012
  - ITINF221: Migració Oracle 10g a Oracle 12c

Fase 4: Propostes de Projectes

- Projectes a llarg termini:

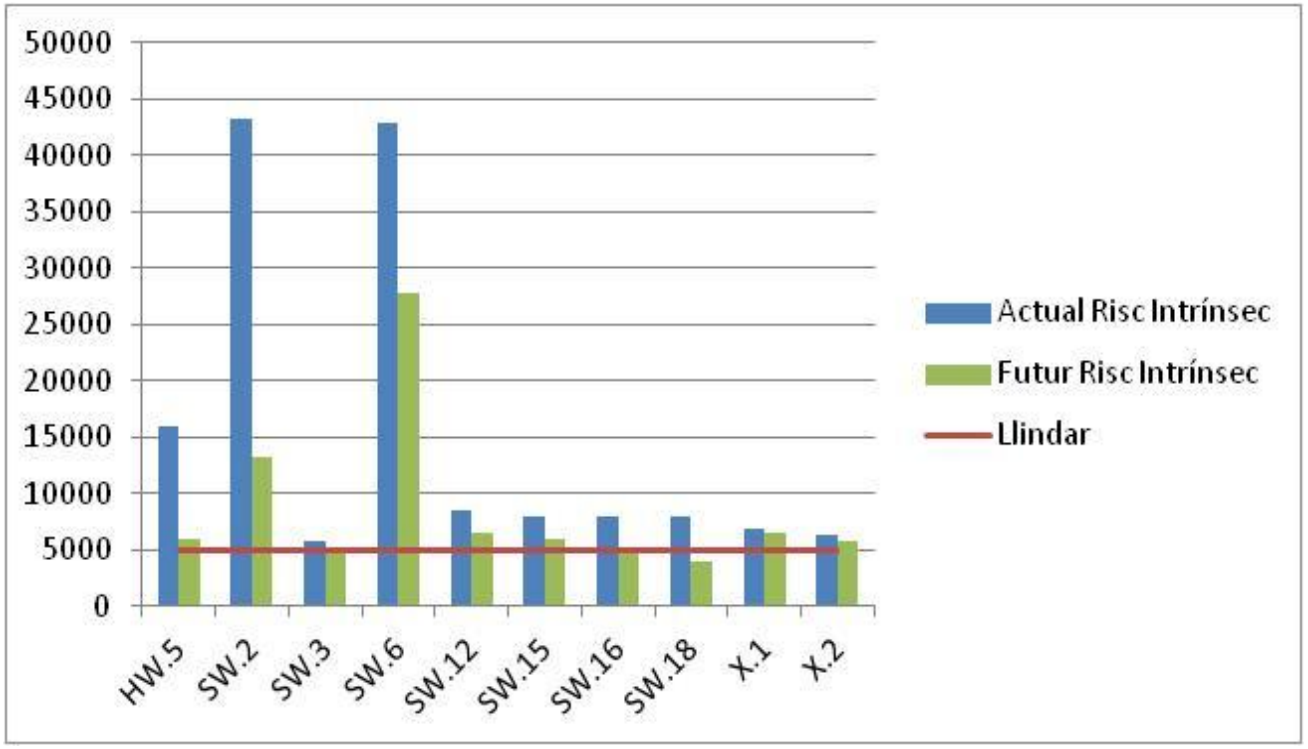
➢ITINF025: Procediments i gestió d'auditories internes i externes.
➢ITINF085: Reestructuració del departament TIC.

Fase 4: Propostes de Projectes

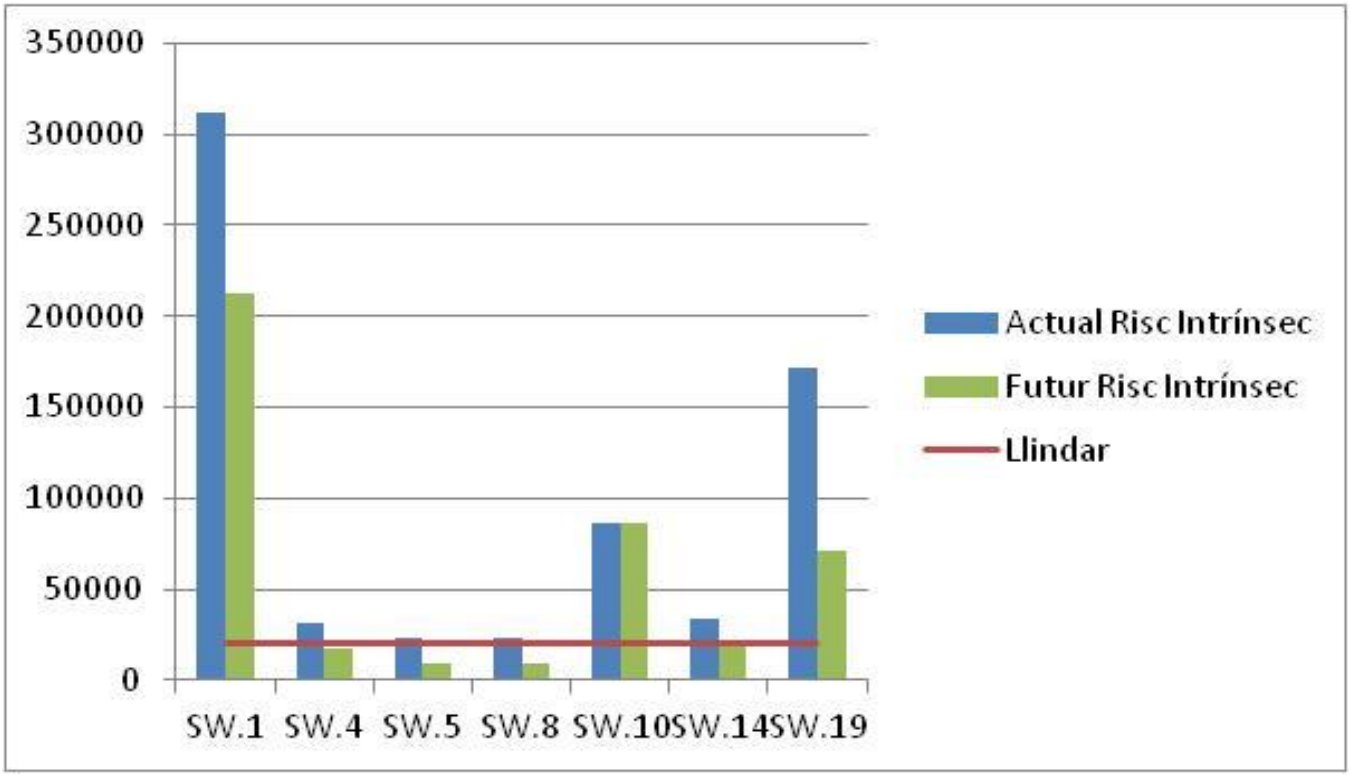
Períodes	Projecte	Duració	Inici	Fi	Cost total
Curt Termini	ITINF105	12 mesos	15/01/2016	31/12/2016	7.460€
	ITINF212	3 mesos	01/04/2016	01/07/2016	1.255€
	ITINF045	6 mesos	01/06/2016	01/12/2016	1.370€
	ITINF150	3 mesos	01/05/2016	01/08/2016	1.760€
	ITINF151	3 mesos	01/07/2016	01/10/2016	1.510€
	ITINF065	8 mesos	01/02/2016	01/10/2016	8.980€
Mig Termini	ITINF068	3 mesos	27/02/2017	27/05/2017	1.530€
	ITINF090	3 mesos	01/03/2017	01/06/2017	1.440€
	ITINF220	6 mesos	01/04/2017	01/10/2017	2.870€
	ITINF221	4 mesos	01/05/2017	01/09/2017	990€
Llarg Termini	ITINF025	6 mesos	01/01/2018	01/06/2018	1.370€
	ITINF085	6 mesos	01/01/2018	01/06/2018	12.050€

42.585 euros

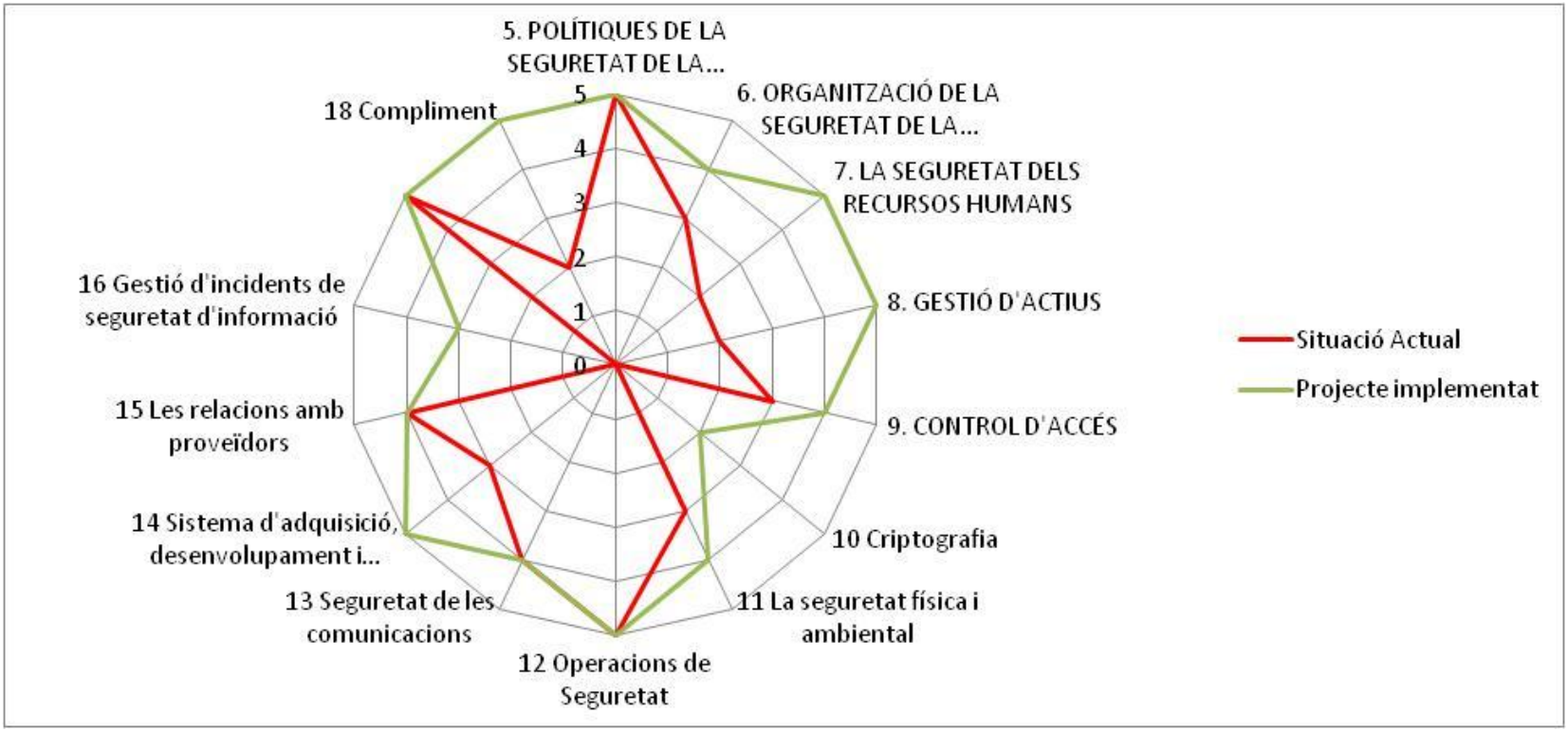
Fase 4: Propostes de Projectes



Fase 4: Propostes de Projectes



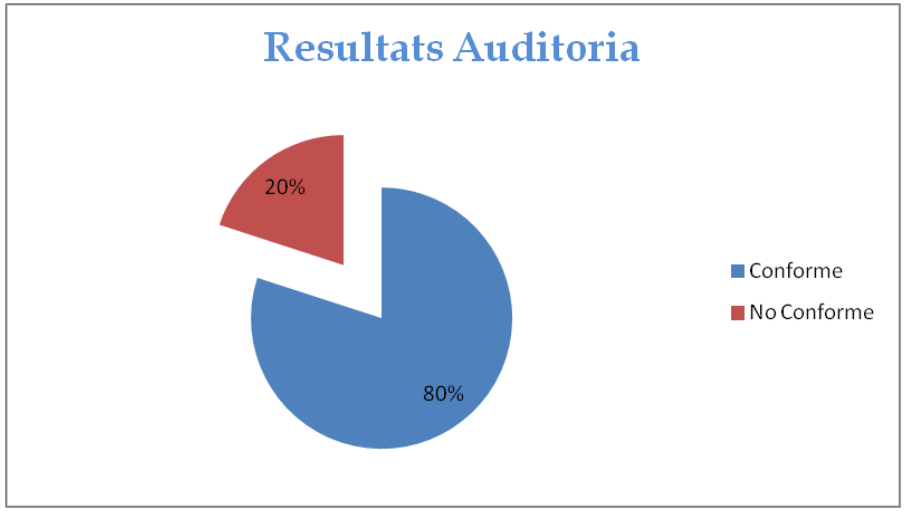
Fase 4: Propostes de Projectes



- Introducció
- Fase 1: Situació actual
- Fase 2: Sistema de Gestió Documental
- Fase 3: Anàlisis de Riscos
- Fase 4: Propostes de Projectes
- **Fase 5: Auditoria de Compliment**
- Conclusions

Fase 5: Auditoria de Compliment

Controls	Conformitats
5.1 Direcció de gestió de seguretat de la informació	Conforme
6.1 Organització interna	Conforme
6.2 Els dispositius mòbils i el teletreball	No Conforme
7.1 Amb anterioritat a l'ocupació	Conforme
7.2 Durant l'ocupació	Conforme
7.3 Terminació i canvi d'ocupació	Conforme
8.1 La responsabilitat dels actius	Conforme
8.2 Classificació de la Informació	Conforme
8.3 Mitjans de manipulació	Conforme
9.1 Els requisits de negoci de control d'accés	No Conforme
9.2 Gestió d'accés dels usuaris	Conforme
9.3 Responsabilitat dels usuaris	Conforme
9.4 Sistema de control i d'accés a les aplicacions	Conforme
10.1 Controls criptogràfics	No Conforme
11.1 Les àrees segures	Conforme
11.2 Equip	No Conforme
12.1 Procediments i responsabilitats operacionals	Conforme
12.2 Protecció contra el malware	Conforme
12.3 Còpia de seguretat	Conforme
12.4 Registre i supervisió	Conforme
12.5 de control de programari operacional	Conforme
12.6 La gestió tècnica de la vulnerabilitat	Conforme
12.7 Sistemes d'informació consideracions d'auditoria	Conforme
13.1 De gestió de seguretat de xarxa	Conforme
13.2 La transferència d'informació	No Conforme
14.1 Els requisits de seguretat dels sistemes d'informació	Conforme
14.2 Seguretat en els processos de desenvolupament i suport	Conforme
14.3 Les dades de prova	Conforme
15.1 Seguretat de la informació en relació amb els proveïdors	No Conforme
15.2 La gestió de la prestació de serveis de proveïdors	Conforme
16.1 Gestió dels incidents de seguretat de la informació i millores	No Conforme
17.1 La continuïtat seguretat de la informació	Conforme
17.2 Les redundàncies	Conforme
18.1 El compliment dels requisits legals i contractuals	Conforme
18.2 Opinions seguretat de la informació	Conforme



Fase 5: Auditoria de Compliment

Àrees	CMM 2016	CMM 2019
5. Polítiques de la Seguretat de la Informació	L5	L5
6.Organització de la seguretat de la informació	L3	L4
7. La seguretat dels recursos humans	L2	L5
8. Gestió d'actius	L2	L5
9. Control d'accés	L3	L4
10.Criptografia	L0	L2
11.La seguretat física i ambiental	L3	L4
12.Operacions de Seguretat	L5	L5
13.Seguretat de les comunicacions	L4	L4
14.Sistema d'adquisició, desenvolupament i manteniment	L3	L5
15.Les relacions amb proveïdors	L4	L4
16.Gestió d'incidents de seguretat d'informació	L0	L2
17.Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	L5	L5
18.Compliment	L2	L4

- Introducció
- Fase 1: Situació actual
- Fase 2: Sistema de Gestió Documental
- Fase 3: Anàlisis de Riscos
- Fase 4: Propostes de Projectes
- Fase 5: Auditoria de Compliment
- **Conclusions**

Conclusions

- Precisar l'estat de la seguretat de la informació actual en relació als diferents aspectes de la Norma.
- Establir una base documental.
- Identificar e inventariar els actius crítics de l'Organització.
- A partir dels riscos trobats, s'han seleccionat i prioritzat un seguit de projectes i mesures que permetran millorar la Seguretat de l'Organització.

Conclusions- línies de treball futur

- Ampliar l'abast d'actius, incloure els actius de la part d'industrial.
- Segon anàlisis de riscos amb els actius de fàbrica i les plantes de producció on tindrem en compte altres tipus d'amenaces als que estem exposats.

Moltes gràcies

Pla Director de Seguretat de la Informació de Traun

Nom Estudiant: Maria Montserrat Ponce León

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

Consultor: Arsenio Tortajada Gallego

Data Lliurament: 06/06/2016