Sistemes de gestió de la seguretat de la informació

Jordi Muñoz

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

TFM - SGSI a la Mutua Interuniversitària

SGSI de la Mutua Interuniversitaria

- FASE 1 Situació Actual.
  - Contextualització i comprensió del entorn.
  - Objectius i anàlisis diferencial del SGSI.

- FASE2. Sistema de Gestió Documental
  - Elaboració de la Política de Seguretat. Declaració d'aplicabilitat i documentació del SGSI.

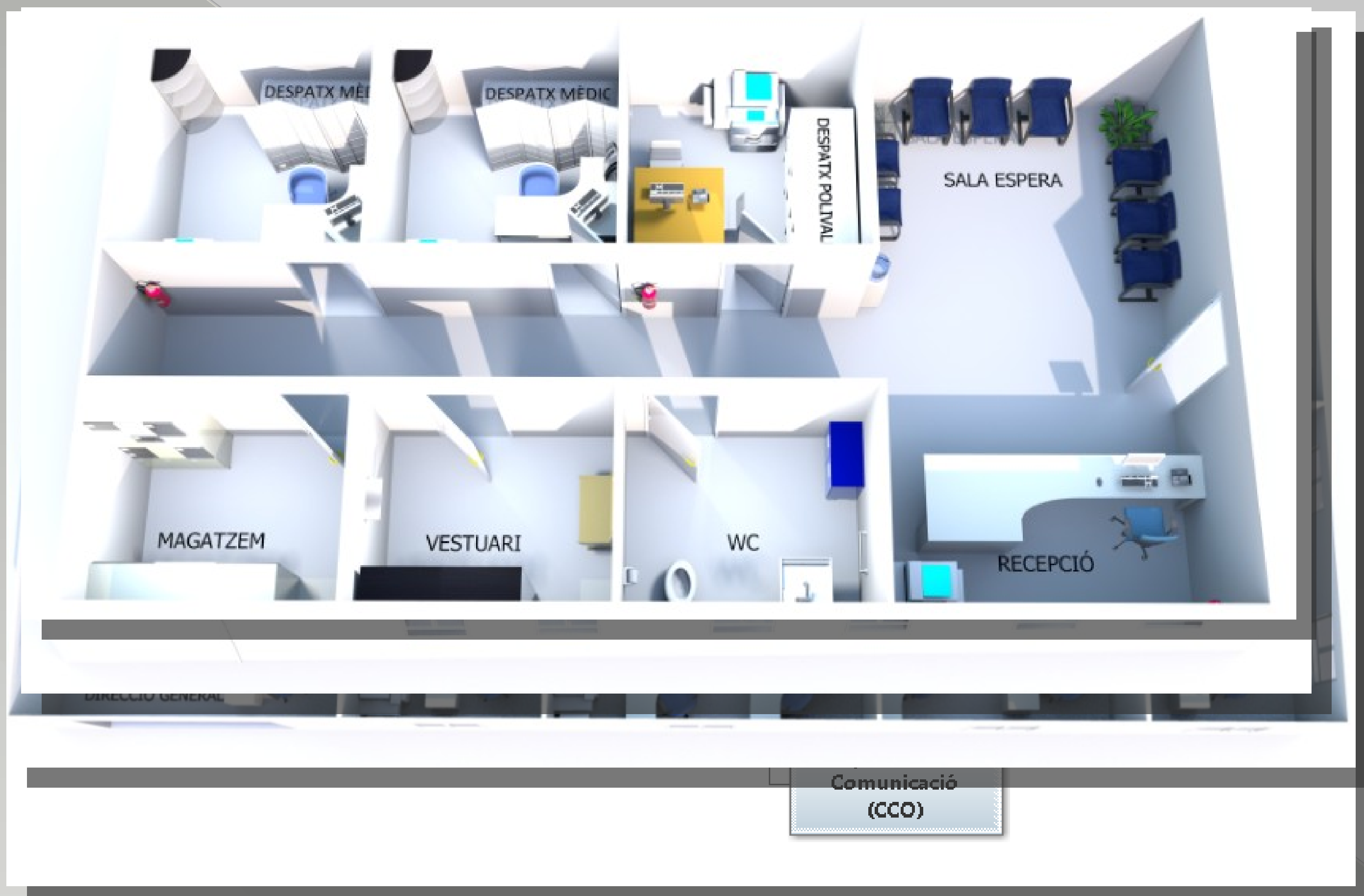
- FASE3. Anàlisis de Riscos.
  - Elaboració d'una metodologia d'anàlisis de riscos, identificació i valoració dels actius, amenaces, vulnerabilitats, càlcul del risc, nivell de risc acceptable i risc residual.
  - Elaboració d'un estudi d'anàlisis de Riscos integrat. (Proposta d'Ampliació).
- FASE4. Proposta de Projectes
  - Avaluació de projectes que ha de portar a terme la Organització per alinear-se amb els objectius plantejats al Pla director.
  - Quantificació econòmica i temporal d'aquests
- FASE5. Auditoria de compliment de la ISO/IEC 27002:2013
  - Avaluació de Controls
  - Avaluació de Maduresa
  - Avaluació del Nivell de compliment
- FASE6. Presentació de Resultats i entrega dels informes
  - Consolidació dels resultats obtinguts durant el procés d'anàlisis.
  - Realització dels informes.
  - Presentació executiva a la Direcció
  - Entrega del projecte final.

FASE 1 Situació Actual. Contextualització.

- Missió
- Historia
- Infraestructures i Equipament
- Objectiu del SGSI
- SOA Inicial
- Pla d'acció

Missió de la Mutua Interuniversitària

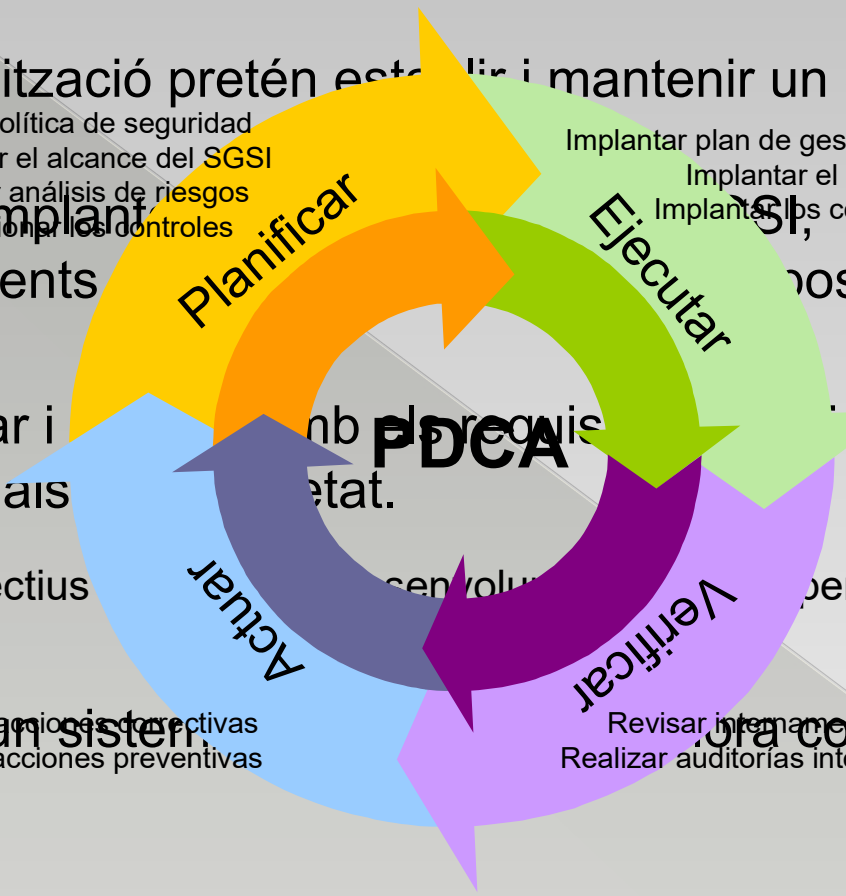
Context Cultura e Historia



DESPATX MÈDIC
DESPATX POLIVAL
SALA ESPERA
MAGATZEM
VESTUARI
WC
RECEPCIÓ
Comunicació
(CCO)

Objectius.

- La Organització pretén est[illegible]lir i mantenir un SGSI documentat.
- Iniciar, implant[illegible] SGSI, assegurar que els procediments [illegible]posta als requisits del sistema.
- Identificar i [illegible]nb els requis[illegible]les obligacions contractuals [illegible]etat.
- Establir objectius [illegible]cen[illegible]per millorar la Seguretat de la Informació
- Establir un sistem[illegible]ora contínua. Cicle PDCA

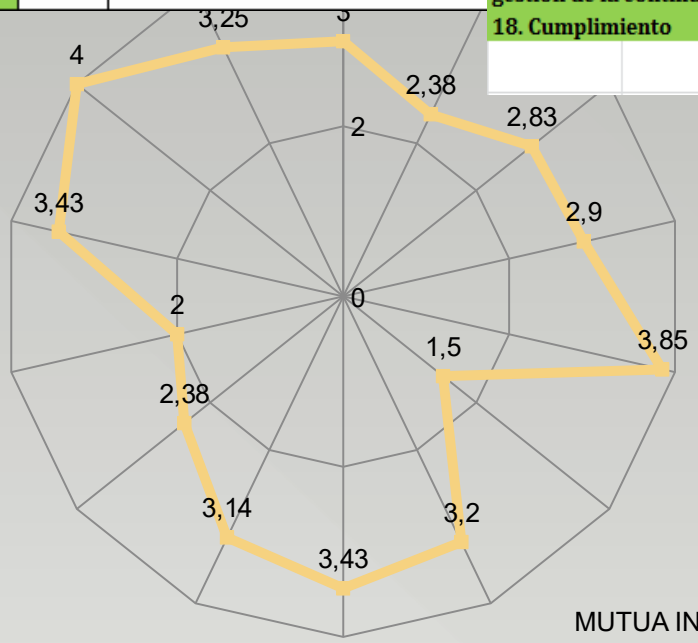


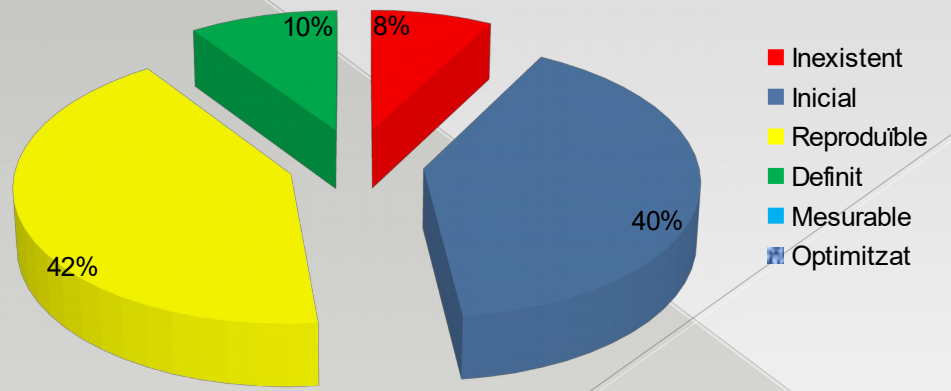
Model de Maduresa Inicial

ISO 27001:2013 Controls

Sección	Control		Total
Políticas de seguridad de la información	5,1	Directrices de gestión de la seguridad de la in	
	5.1.1	Políticas para la seguridad de la información	
			4,00
	5.1.2	Revisión de la política de seguridad de la infor	
			2,00
			6,00
			3,00

5. Políticas de seguridad de la información	Total sección 5	3,00
6. Organización de la seguridad de la informació	Total sección 6	2,38
7. Seguridad relativa a los recursos humanos	Total sección 7	2,83
8. Clasificación de la información	Total sección 8	2,90
9. Control de Acceso	Total sección 9	3,85
10. Criptografia	Total sección 10	1,50
11. Seguridad física y del entorno	Total sección 11	3,20
12. Seguridad de las operaciones	Total sección 12	3,43
13. Seguridad de las comunicaciones	Total sección 13	3,14
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	Total sección 14	2,38
15. Relación con proveedores	Total sección 15	2,00
16. Gestión de incidentes de seguridad de la información	Total sección 16	3,43
17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Total sección 17	4,00
18. Cumplimiento	Total sección 18	3,25
	Total secciones	**2,95**





Punts clau de la SGSI?

- Mesurar, evaluar i tractar els Riscos sobre els actius de la Mutua Interuniversitaria.
- Establir les mesures de seguretat necessaries per Asegurar la correcta gestio de la Seguretat i preservar la Confindencialitat, Disponibilitat e Integritat de la Informació
- Implementar un sistema de Millora Continua de la Seguretat (PDCA), mitjançant l'establiment de controls e indicadors que ens permetin avaluar la eficacia de les mesures de forma continua.
- Capacitar a les persones involucrades en el Sistema per preservar la Seguretat.

Abast

“Centre de Procés de dades i la seva gestió operativa, així com el servei d’atenció al Usuari (SAU) de la Seu de Barcelona de Mutua Interuniversitària.”

Els límits de l’abast del present SGSI s’emmarquen dins de l’activitat de la Organització que és:

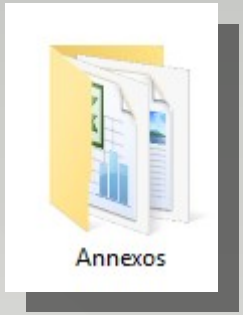
- Serveis d’Asistencia sanitària al personal Universitari
- Gestió de Clients i Treballadors.

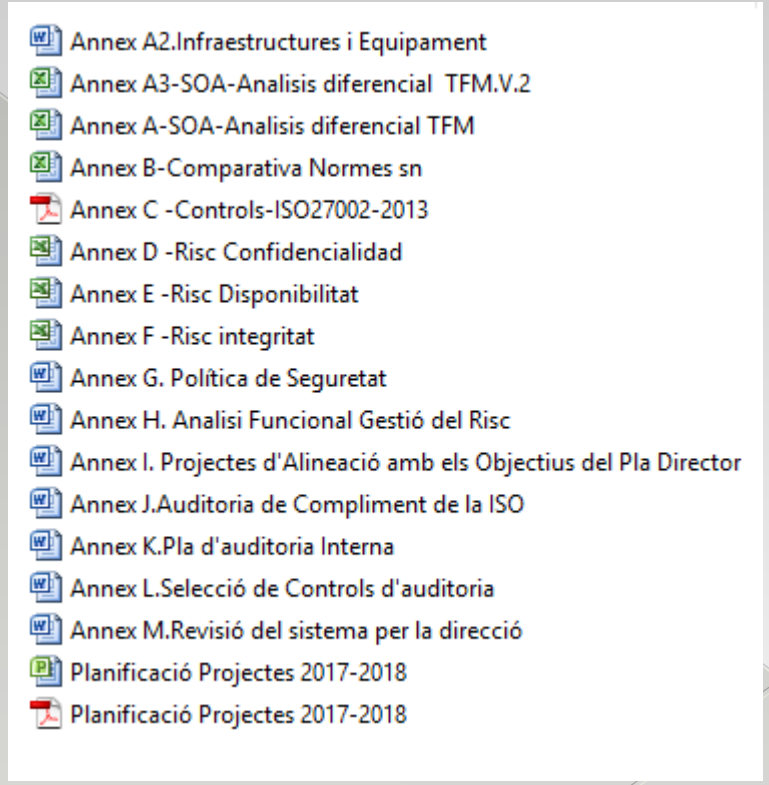
FASE2. Sistema de Gestió Documental

- Política de seguretat
- Auditories Internes
- Pla d'Auditoria
- Gestió d'Indicadors
- Revisió per la direcció
- Rols i Responsabilitats
- Metodologia d'analisis de riscos
- SOA

SISTEMA DE GESTIO DOCUMENTAL

- Un fitxer amb la memòria del projecte
- Un directori amb els annexos.





POLITICA DE SEGURETAT

Fa referencia al punt 5.2 de la norma 27001:2013 també al punt 5.2 de la 14001:2015 i de la 9001:2015.

BASES DE LA POLITICA DE SEGURETAT DE MUTUA INTERUNIVERSITARIA

- Proporcionar als empleats un entorn de treball disponible i fiable respecte a les eines informàtiques, dades i comunicacions d'acord amb les directrius obtingudes del pla estratègic de la organització
- Gestionar adequadament la seguretat de la informació per tal de permetre als seus responsables implantar-hi i mantenir-hi la Organització
- Assegurar la disponibilitat, confidencialitat, e integritat de les dades sanitàries dels treballadors protegits així com de les empreses mutualistes
- Enfortir la relació de confiança de clients i treballadors amb la Organització
- Contribuir a la obtenció de millors nivells d'excel·lència de gestió en la Organització així com de millora de la imatge.
- Complir amb la legalitat aplicable

Proporcionar als empleats un entorn de treball disponible i fiable respecte a les eines informàtiques, dades i comunicacions d'acord amb les directrius obtingudes del pla estratègic de la organització

Gestió D'indicadors

- Avaluar l'eficàcia dels controls
- Es revisaran anualment
- S'implanten un total de 88 indicadors
- Permeten buscar solucions a deficiències
- Es planifiquen i calenderitzen < 5 per setmana.
- Les mesures amb resultat negatiu, impliquen una acció correctiva o preventiva

FASE3. Anàlisis de Riscos.

- Gestió del Risc
- Magerit
- Analisi dels actius rellevants
- Taula de valoració en tres dimensions
- Estudi d'amenaces
- Avaluació del Risc e impacte sobre el SI
- Salvaguardes
- Risc Efectiu

ANALISIS DE RISCOS?

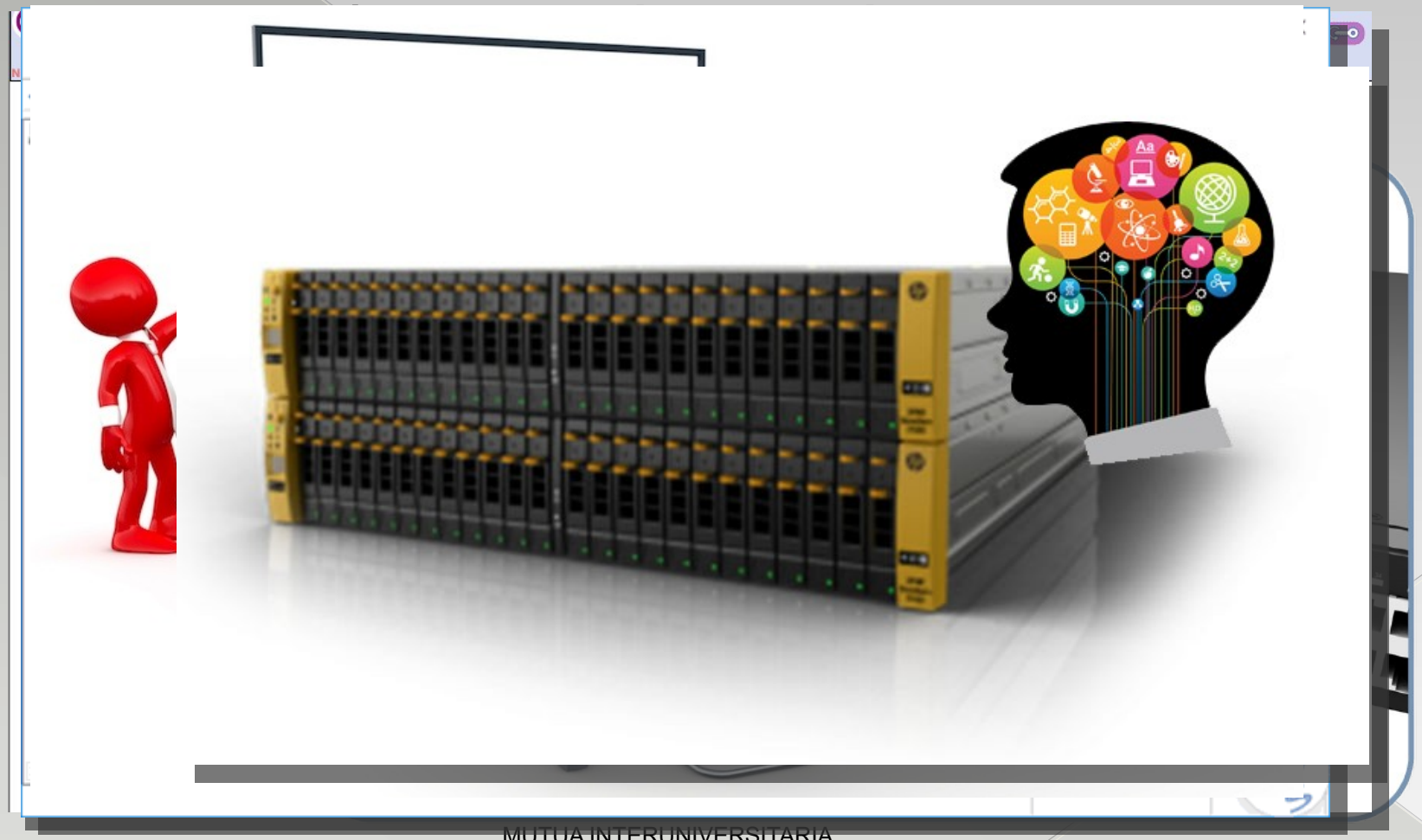
Risc Efectiu per Dimensió

		SALVAGUARDES-AMENACES : DIMENSIÓ CONFIDENCIALITAT				1
VALOR ECONÓMIC	COS SALVAGUARDA	SALVAGUARDES	Averia de hardware			
			Dism. Vulner.	Dism. Impacte	Relacionada	
2.500 €	Medio	Salvaguardes relacionades amb la Política de seguretat de la informació	Baja	Baja	S	
6.000 €	Alto	Salvaguardes relacionades amb la Estructura per la seguretat de la informació			N	
2.500 €	Medio	Salvaguardes relacionades amb la Seguretat dels accessos de terceres parts	Baja	Baja	S	
6.000 €	Alto	Salvaguardes relacionades amb la Externalització (outsourcing)	Baja	Baja	S	
600 €	Bajo	Salvaguardes relacionades amb la Responsabilitat sobre els actius	Media	Baja	S	
0 €	Nulo	Salvaguardes relacionades amb la Classificació de la informació			N	
2.500 €	Medio	Salvaguardes relacionades amb la Seguretat en la definició del treball i els recursos			N	
6.000 €	Alto	Salvaguardes relacionades amb la Formació dels usuaris	Baja	Baja	S	
2.500 €	Medio	Salvaguardes relacionades amb la Resposta devant d'incidències i mals funcionaments de la seguretat	Baja	Baja	S	
18.000 €	Muy alto	Salvaguardes relacionades amb les Arees segures			N	
18.000 €	Muy alto	Salvaguardes relacionades amb la seguretat dels equips.	Media	Baja	S	
6.000 €	Alto	Salvaguardes relacionades amb els controls generals			N	
2.500 €	Medio	Salvaguardes relacionades amb els procediments i responsabilitats d'operació	Media	Baja	S	
6.000 €	Alto	Salvaguardes relacionades amb la planificació i acceptació del sistema			N	
18.000 €	Muy alto	Salvaguardes relacionades amb la protecció contra el software malicios.			N	
6.000 €	Alto	Salvaguardes relacionades amb la gestió interna de suports i recuperació			N	

60.000 €	formac	Grup de Dades de Gestio Comercial	0,00	0,00	17,98	466,20
200.000 €	formac	Grup de Dades de Gestió de RRHH	0,00	0,00	59,94	1.998,00
200.000 €	formac	Grupo de Dades de Direcció	0,00	0,00	59,94	1.998,00
6.000 €	Serveis	Serv.infraestructures i manteniment T.I	0,00	0,00	1,40	46,62
60.000 €	Serveis	Serv. Aplicacions T.I	0,00	0,00	17,98	599,40
60.000 €	Serveis	Serv. Consultores y Projectes	0,00	0,00	17,98	599,40

FASE4. Proposta de Projectes

- Projectes d'alineació amb el Pla director



FASE5. Auditoria de compliment de la ISO/IEC 27002:2013

- Auditoria de compliment de la ISO
- Pla d'auditoria
- Preparació de l'auditoria – selecció de controls
- Procés d'auditoria
- Resum dels resultats d'auditoria

PROCÉS D'AUDITORIA

- Resultats de l'Auditoria

CONTROLS	SECCIONS	ANT	ACT
5. Políticas de seguridad de la información	Total sección 5	3,00	4,50
6. Organización de la seguridad de la informació	Total secció 6	2,38	3,38
7. Seguridad relativa a los recursos humanos	Total secció 7	2,83	4,17
8. Clasificación de la información	Total secció 8	2,90	4,70
9. Control de Acceso	Total secció 9	3,85	5,00
10. Criptografia	Total secció 10	1,50	3,50
11. Seguridad física y del entorno	Total secció 11	3,20	4,33
12. Seguridad de las operaciones	Total secció 12	3,43	4,29
13. Seguridad de las comunicaciones	Total secció 13	3,14	4,57
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	Total secció 14	2,38	4,15
15. Relación con proveedores	Total secció 15	2,00	3,60
16. Gestión de incidentes de seguridad de la información	Total secció 16	3,43	4,71
17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Total secció 17	4,00	5,00
18. Cumplimiento	Total secció 18	3,25	4,50
	Total Seccions	2,95	4,31

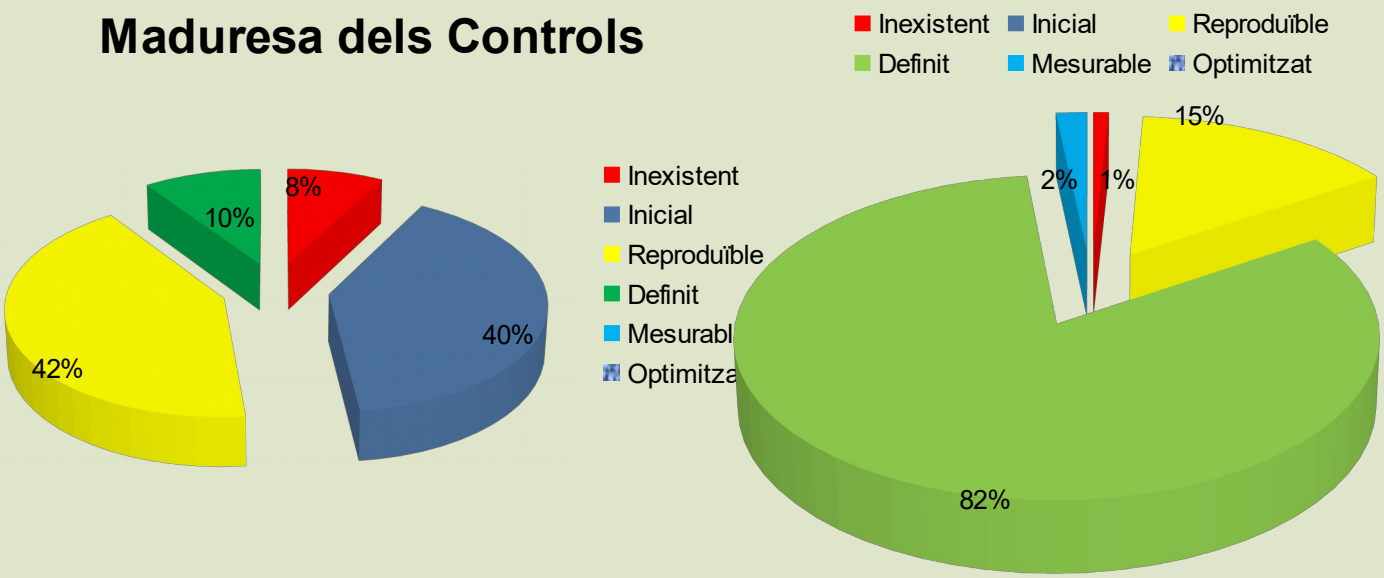
MUTUA INTERUNIVERSITARIA

En la present auditoria de Compliment de la ISO/IEC 27001:2013, s'han detectat un total de 10 Desviacions, 3 Opcions de Millora i un 1 Punt fort.

FASE6. Presentació de Resultats i entrega dels informes

- Revisió del sistema per la direcció
- Conclusions finals
- Presentació TFM

Revisió del sistema per la direcció



Estat
INICIAL

Estat
DEFINIT

- Amb un Risc Efectiu de: 692,78 €
- Destruccions de la informació:
  - Amb un Risc Efectiu de: 689,93 €

CONCLUSIONS FINALS

- S'ha posat en marxa el cicle PDCA de la SGSI
- S'han complert les expectatives de la direcció i l'alineació del Pla director amb els objectius de la direcció.
- S'han portat a terme els objectius definits mitjançant els projectes desenvolupats, s'ha assolit el resultat esperat en la planificació dels projectes.
- Un gran número de controls ja es troben en marxa i tenen indicador per la avaluació del mateix.
- S'ha millorat l'estat de maduresa d'un estat inicial a un estat Definit.
- S'ha involucrat i format al personal involucrat en el Sistema de Gestió
- La Organització ha entès el SGSI i existeix una intenció de la direcció en seguir recolzant el Sistema.
- S'han avaluat i acceptat els Riscos efectius per dimensions
  - Risc Confidencialitat: 14.000
  - Risc Disponibilitat: 15.000
  - Risc Integritat: 7000
  - Màxim Risc Efectiu acceptat per amenaça en totes les dimensions:
    Llindar 3000€
- L'Objectiu a curt i mig termini és desenvolupar i enfortir el sistema actual
- El sistema ha demostrat la seva eficàcia i compleix amb els requisits establerts per les normes de referència aplicades

Gràcies!
Precs i preguntes

TFM.MISTIC UOC.2017