MISTIC – Màster Universitari de Seguretat de les TIC. TREBALL FINAL DE MASTER - ISO/IEC 27001:2013

Jordi Muñoz Nieto
Arsenio Tortajada Gallego

Universitat Oberta de Catalunya - Març 2017

C) Copyright

Control de Versions del Document.

Versió	Data
TFM.V1	08/03/2017
TFM.V1.2	10/03/2017
TFM.V2.1	13/03/2017
TFM.V2.2	15/03/2017
TFM.V2.3	20/03/2017
TFM.V.2.4	21/03/2017
TFM.V.2.5	22/03/2017
TFM.V.2.6	23/03/2017
TFM.V.3.1	29/03/2017
TFM.V.3.2	31/03/2017
TFM.V.3.3	03/04/2017
TFM.V.3.4	05/04/2017
TFM.V.3.5	10/04/2017
TFM.V.3.6	12/04/2017
TFM.V.4.1	20/04/2017
TFM.V.4.2	24/04/2017
TFM.V.4.3	24/04/2017
TFM.V.4.6	27/04/2017
TFM.V.5.1	02/05/2017
TFM.V.5.2	08/05/2017
TFM.V.5.3	09/05/2017
TFM.V.5.6	15/05/2017
TFM.V5.7	17/05/2017
TFM.V6.1	20/05/2017
TFM.V6.2	27/05/2017
TFM.V6.3	03/06/2017
TFM.V6.4	**05/06/2017**

DEDICATORIA I AGRAIMENTS.

Al Toni Serra que em fa cada dia una mica millor professional i millor persona.

Als meus companys Toni i Vicen que sense la seva paciència i suport no hagués estat possible.

Als meus amics i familiars que durant tantes hores hem estat molt lluny i molt aprop.

Sense vosaltres això no seria possible. Gràcies a tots per ser-hi!

1. RESUM DEL TREBALL

Aquest Projecte planteja l'establiment de les bases per portar a terme la implementació d'un SGSI (Sistema de Gestió de la Seguretat de la informació), en base a la Normativa Internacional de Referència ISO/IEC 27001:2013.

Aquest es prenent englobar en un Sistema Integral de Gestió d'una empresa fictícia anomenada Mutua Interuniversitària. Totes les dades tant de l'empresa com del entorn físic o ubicació de la mateixa son dades fictícies emprades per portar a terme aquest treball.

Per portar a terme el treball s'abordaran les següents fases:

FASE 1 Situació Actual.
- Contextualització i comprensió del entorn.
- Objectius i anàlisis diferencial del SGSI.
- Anàlisi i disseny, d'aspectes Comuns directes i col·laterals de les diferents normes del Sistema Integral de Gestió (Proposta d'ampliació)

FASE2. Sistema de Gestió Documental
- Elaboració de la Política de Seguretat. Declaració d'aplicabilitat i documentació del SGSI.
- Estudi d'un sistema integrat de Gestió Documental (Proposta d'ampliació)

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
- Anàlisis de Projectes d'integració dels Sistemes de Gestió (Proposta d'Ampliació)

FASE5. Auditoria de compliment de la ISO/IEC 27002:2013
- Avaluació de Controls
- Avaluació de Maduresa
- Avaluació del Nivell de compliment
- Estudi d'integracio´ d'Auditories del Sistema Integrat de Gestio´ (Proposta d'Ampliació)

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.
- Estudi de viabilitat dels resultats d'integració dels sistemes de Gestió (Proposta d'Ampliació)

2. SUMMARY

This project proposes the establishment of bases for carrying out the implementation of an ISMS (System Management Information Security), based on the International Regulations Reference ISO/IEC 27001: 2013.

This will include taking a comprehensive management system for a fictitious company called Mútua Interuniversitària. All the data from both the company and the physical environment or location of the same dummy data are used to carry out this work.

To carry out the work will address the following phases:

PHASE 1 Current Situation.

- Understanding of the context and environment
- Objectives and differential analysis of ISMS.
- Analysis and graphing, Common direct and collateral of the different standards of Integrated Management (Proposed extension)

FASE2. Document Management System

- Development of Security Policy. Declaration of applicability of the ISMS documentation.
- Study of an integrated Document Management (Proposed extension)

PHASE 3. Risk Analysis.

- Developing a methodology for risk analysis, identification and evaluation of assets, threats, vulnerabilities, risk calculation, level of acceptable risk and residual risk.
- Elaboration of a study of integrated risk analysis. (Proposed Extension).

FASE4. Proposed Projects

- Evaluation of projects that should lead to the Organization for Terma line with the objectives set in the Master Plan.
- Quantification of these temporary economic and
- Analysis Project Integration Management Systems (Proposed Expansion)

PHASE 5. Audit of compliance with ISO / IEC 27002: 2013

- Controls Assessment
- Maturity Assessment
- Evaluation of the level of compliance
- Study Audits integration of Integrated Management System (Proposed Expansion)

FASE6. Earnings and delivery reports

- Consolidation of the results obtained during the analysis process.
- Completion of Report
- Presentation to Executive Management
- Delivery of the final project.
- Feasibility study of the results of integration of systems management (proposed extension)

INDEX

3. FASE1 SITUACIÓ ACTUAL. CONTEXTUALITZACIÓ, COMPRENSIÓ DEL ENTORN Y ANALISI DEL CAS D'ESTUDI

3.1. DESCRIPCIÓ DETALLADA DE LA ORGANITZACIÓ.

3.1.1. MISIÓ

La organització sobre la que implementarem el SGSI, és del sector de les Mútues Mèdiques que tindrà com a missió donar servei al personal Universitari de les universitats adherides a la mateixa, tant a nivell sanitari pel personal docent que hi treballa, com d'assegurança de reemborsament pels estudiants.

Fins el moment les universitats adherides son la UOC, la UAB i la Universitat Rovira i Virgili. Els serveis que aporta la Organització als clients adherits son:

- Servei d'urgències.
- Assistència Sanitaria
- Malaltia comú a nivell de control.

Els estudiants que degut a alguna malaltia demostrada i acreditada per un facultatiu perdessin una convocatòria podrien rebre un reemborsament per part de la Mutua Interuniversitària per tal de fer front al pagament de la matricula.

3.1.2. CONTEXT I ANÀLISI DE LA COMPETENCIA.

El context de la Mutua Interuniversitària es troba englobat dins del àmbit de les Mútues d'accidents de treball, aquestes son empreses que col·laboren amb la seguretat Social, mitjançant una associació privada d'empresaris constituïda mitjançant l'autorització del Ministeri de Treball i la Seguretat Social, e inscrites en el Registre especial i depenent d'aquest. Aquestes tenen per finalitat col·laborar en la gestió de la Seguretat Social sota la direcció i tutela del mateix, sense ànim de lucre i assumint els seus associats i responsabilitat mancomunada en els supòsits i abast establert per la llei. La gestió de la qual es en base a pressupostos autoritzats i controlats pels ministeris d'Hisenda i de la Seguretat Social.

3.1.3. CULTURA

En l'àmbit soci cultural la Mutua Interuniversitària es destaca per la rectitud del seu codi ètic en la gestió del patrimoni públic. Per altre banda a nivell intern és bàsic per la Mutua el fet de que la comunicació entre els departaments sigui fluida i estableix plans i projectes de col·laboració per optimitzar esforços.

La definició dels processos i la capacitació de transversalitat dels mateixos per alinear-se amb totes les parts del negoci, son tasques que s'impulsen des de direcció i en les que s'inverteixen grans esforços i recursos.

En l'àmbit econòmic, la Mutua Interuniversitària destaca per la transparència total dels seus comptes i la publicació dels salaris dels seus directius en la pròpia web.

En l'àmbit tecnològic la Mutua Interuniversitària destaca per encapçalar projectes de millora continua de les aplicacions del sector tant a nivell funcional, d'innovació, d'integració dels seus Sistemes de Gestió, així com de nivell de securització dels entorns.

3.1.4. HISTORIA DE LES MUTUES D'ACCIDENTS DE TREBALL

Les mútues d'accidents de treball son Mútues Col·laboradores amb la Seguretat Social. Dins d'aquest àmbit és on es troba la Mutua Interuniversitària.

Les mutues colaboradores amb la seguretat social tenen els seus precedents en el segle XII, els seus inicis a la llei d'accidents de treball del any 1900, on el patró es veu obligat a indemnitzar als treballadors accidentats amb independencia de la culpa empresarial, fins a les últimes modificacions realitzades a les últimes decades de la democracia.

Els origens de les Mutues Actuals es remonten a les institucions de estructura mutualista que havien vingut funcionant desde el segle XII, fonamentalment "Hermandades de Socorro Mutuo", "Montepíos" i "Cofradias".

Entre 1900 i 1921 apareixen 18 Mútues d'Accidents de treball. Les normes reglamentaries de desenvolupament de la Llei d'accidents de treball conferia a les mútues d'accidents de treball el caràcter d'entitats acceptades com asseguradores del risc d'accident de treball juntament amb les societats mercantils d'assegurances. Les antigues Mútues d'accidents de treball actuaven amb caràcter voluntari i els seus principis de funcionament es basaven en les antigues institucions mutualistes.

Al 2013 fruit de la fusió de dos mútues imaginaries es fundarà la Mutua Interuniversitària, de caràcter social i altruista, basada en un esperit cooperativista i sense ànim de lucre, amb una mentalitat basada en l'ètica professional, social i salarial, sobre la que treballarem en aquest projecte.

3.1.5. MITJANS.

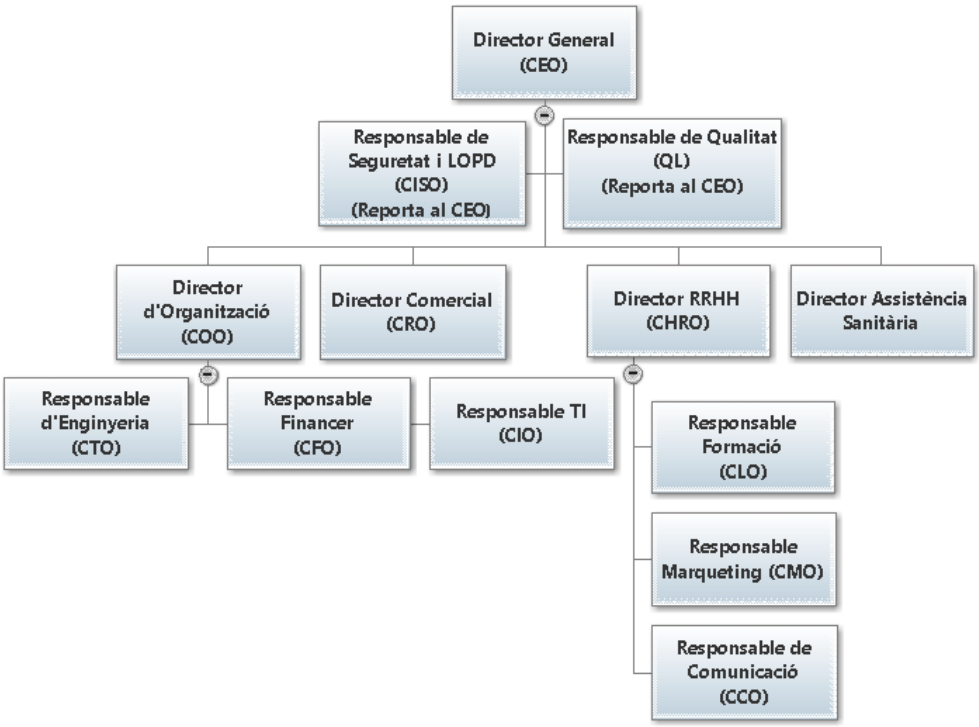
L'empresa compta amb 250 empleats distribuïts en personal Administratiu, Sanitari, Directiu i personal de Suport a la organització. Es disposa també de servei d'Ambulància i taxi, autoritzat pels serveis Mèdics.

Els departaments de la Organització son:

- Direcció General
- Departament Organització
- Assistència Sanitària,
- Recursos Humans,
- Recursos Econòmics.
- Gestió de Client
- Departament de Sistemes, Seguretat, TICs
- Qualitat i Medi Ambient
- LOPD
- Enginyeria.

Diagrama funcional.

A continuació mostrarem el diagrama funcional de la organització establert de mode jeràrquic.



3.1.6. LOCALITZACIÓ I HORARIS

La Mutua Interuniversitària a està distribuïda en una Seu Central a Barcelona on es desenvolupen les tasques Administratives, Organitzatives, funcionals i de Gestió, que també alberga el CPD principal.

- Centre de Barcelona, ubicat al Carrer Aragó 123

Per altre banda tenim una sucursal a Manresa on s'allotja el centre de Contingència amb el CPD alternatiu, i totes les màquines replicades. No obstant encara que no es tracti d'una sucursal administrativa si que s'hi desenvolupen tasques d'atenció sanitària.

- Centre de Manresa, ubicat al Carrer Major número 3

El nombre de facultatius i personal depèn de cada un dels centres. I l'horari es de 8h a 20h.

Per altre costat es disposa de tres dispensaris, un dispensari complert a cadascuna de les universitats adherides actualment.

- Dispensari UOC, ubicat a la rambla del poble nou numero 9
- Dispensari Rovira i Virgili, ubicat al carrer del escorxador s/n.
- Dispensari Universitat Autònoma, ubicat a la plaça Cívica.

Tots tres es troben a peu de carrer, en un local en planta baixa.

3.1.6.1. EQUIPACIONS I EQUIPAMENTS.

Adjunt a la memòria del projecte afegim l'annex A2. Infraestructures i Equipaments on definirem les Infraestructures i Equipament de la Seu Central, Sucursal i Dispensari de la Organització així com la estructura del CPD i del centre de Contingència.

Es mostrarà una taula especificant les característiques dels mateixos així com un planell a escala i una imatge renderitzada del mateix en 3d.

Podrem trobar la definició acurada de cadascun dels equipaments per localització de treball.

- INFRAESTRUCTURA DE LA SEU CENTRAL
- INFRAESTRUCTURA TÉCNICA DE LA SEU CENTRAL
- INFRAESTRUCTURA DE LA SUCURSAL DE MANRESA I CENTRE DE CONTINGÈNCIA.
- INFRAESTRUCTURA D'UN DISPENSARI

3.2. OBJECTIU SGSI

La Organització pretén establir i mantenir un SGSI documentat e integrar-lo a la vegada amb el seu Sistema de Gestió Integrat de Qualitat i Medi Ambient, per portar-ho a terme a d'identificar els actius a protegir, l'enfoc de la gestió del risc adoptat per la organització, els objectius i controls així com el grau de protecció requerit.

La organització ha de determinar i proporcionar els recursos necessaris per iniciar implantar i mantenir el SGSI, així com assegurar que els procediments de seguretat donen resposta als requisits del sistema. Identificar i complir amb els requisits legals i les obligacions contractuals de seguretat,

La direcció de la Organització aprovarà formalment la implementació del SGSI.

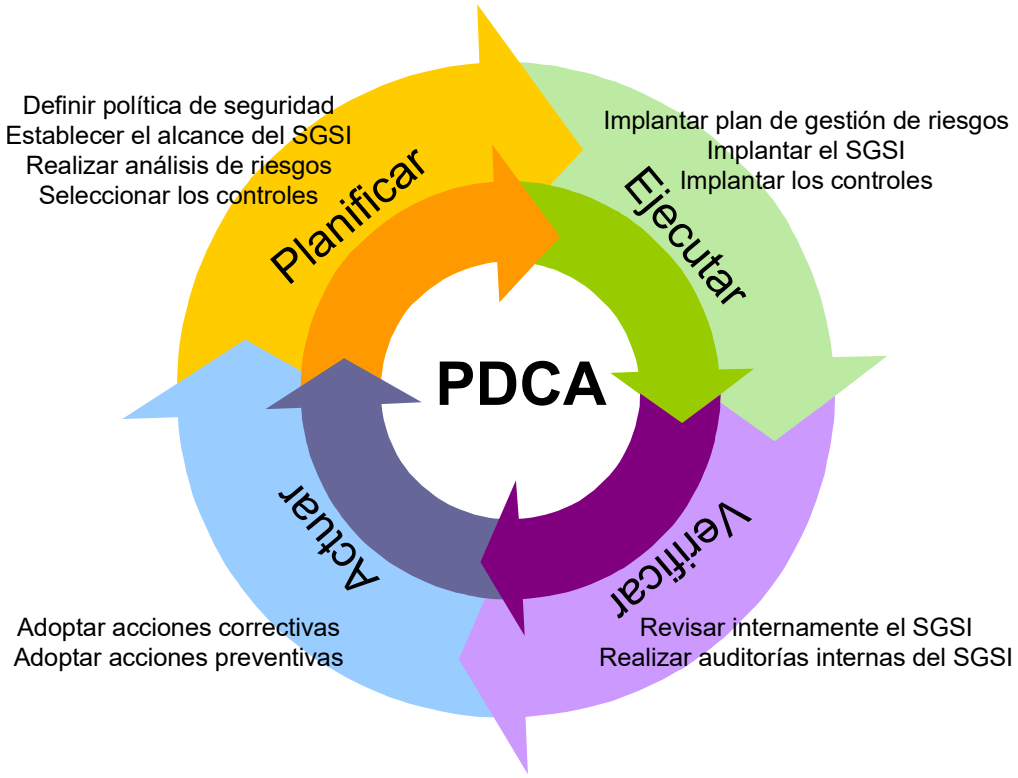
Per tal d'establir un Anàlisi de compliment inicial de la organització vers l'SGSI desenvolupem una taula de mesura que adjuntarem amb l'Annex A del present document. I del qual podrem extreure l'anàlisi diferencial amb l'SGSI i unes primeres intuïcions de l'estat de maduresa de la organització vers la seguretat.

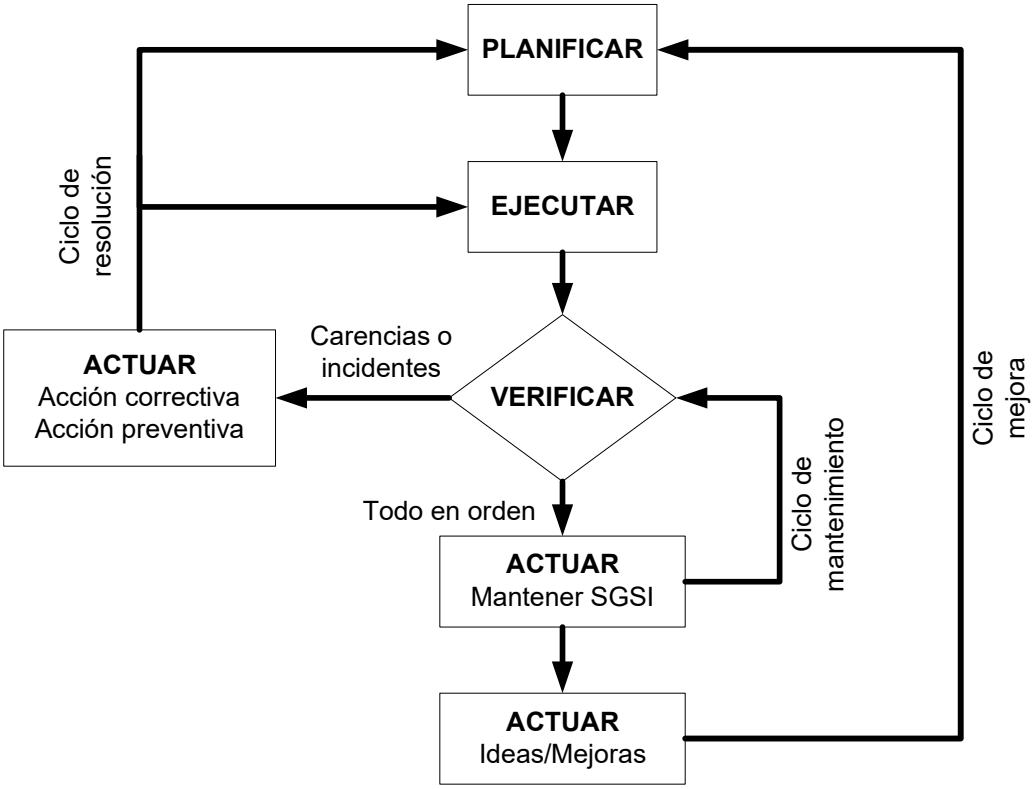
3.3. PLA D'ACCIÓ.

El pla d'acció que es portarà a terme per definir la SGSI serà el següent.
En primer lloc per identificar i documentar l'abast i els objectius del SGSI es cobriran els següents aspectes que mostrarem a continuació.

a) La Organització definirà la política de seguretat.

b) La Organització definirà l'abast del SGSI, els seus límits hauran de ser definits en termes de les característiques de la organització, localització actius i tecnologies.
c) La organització Abordarà un anàlisis de Riscos proporcionat a la natura i valoració dels actius, i dels riscos als que estan exposats. La valoració del risc identificarà les amenaces que poden comprometre els actius, la seva vulnerabilitat i possible impacte en la organització. Determinant el nivell de risc.
d) Els Riscos que es gestionaran estaran identificats basant-se en la política de la Organització sobre la seguretat de la informació i en el grau de seguretat requerit* En una primera instància ja que pretenem desenvolupar en propers punts un sistema integrat de gestió on la anàlisis de riscos haurà de ser realitzat d'una forma conjunta i s'haurà de considerar com reverteix la gestió d'un risc en una dimensió i norma sobre l'altre.
e) La direcció aprovarà els riscos residuals.
f) La organitzacio´ seleccionara` de la ISO/IEV 27002:2013 els controls adequats, d'acord amb els objectius que es pretenen obtenir amb els mateixos, justificant la selecció.
g) La Organitzacio´ si ho considera necessari, seleccionara` controls específics addicionals fora de la 27002:2013, adequats al model particular del negoci de la Organització, així´ com els objectius que es pretenen obtenir amb els mateixos, justificant-ne la selecció. Podem trobar un quadre resum dels controls al Annex C adjunt a aquest document.
h) La Organitzacio´ preparara` una relacio´ dels controls que son aplicables per a aconseguir el nivell de risc residual aprovat per la direcció.
i) Aquests aspectes es revisaran periòdicament en funció de les necessitats
j) Aquest SGSI adaptarà el model conegut com PDCA (Planificar, Fer, Verificar i Actuar), en la següent figura mostrarem la sèrie de fases de millora continua basades en aquest model.




PLANIFICAR
EJECUTAR
VERIFICAR
ACTUAR
Acción correctiva
Acción preventiva
Carencias o
incidentes
Todo en orden
ACTUAR
Mantener SGSI
ACTUAR
Ideas/Mejoras
Ciclo de
resolución
Ciclo de
mantenimiento
Ciclo de
mejora

3.4. ABAST DEL PLA DIRECTOR DE SEGURETAT

L'Abast del Pla director de seguretat és el següent.

"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.

Aquests seran els actius de negoci que s'han pres com a base de referencia.

Els actius que estan dins de l'abast del SGSI; estan situats a la seu central de la Organització ubicada a Barcelona al Carrer Aragó 123, i en el centre de contingència ubicat a Manresa al Carrer Major número 3.

Tots els actius es trobaran detallats i documentats al document d'anàlisis de risc i ubicats dins de cada actiu de negoci descrits en el mateix.

Les persones que estan directament implicades en la gestió del SGSI son 20, entre tècnics, Auditors i direcció dels diferents departaments involucrats.

Exclusions del Abast.
Existeixen un total de tres centres sanitaris distribuïts en Barcelona, Girona i Manresa que en primera instància es trobaran fora del abast del present pla director.

També estaran exclosos del àmbit els dispensaris ubicats a les universitats i els centres concertats amb tercers que puguin donar servei en casos en que s'ampliïn els contractes amb universitats externes a l'àmbit o zona d'actuació.

Futures ampliacions de l'Abast.
Com a futures ampliacions de l'Abast, podríem incloure tant l'auditoria del centre de contingència de Manresa, així com la Sucursal de Girona.
Per altre banda també podríem incloure la Gestió Sanitaria i/o Administrativa de tota la organització en totes les seves ubicacions.

3.5. OBJECTIUS I ANALISIS DIFERENCIAL DEL SGSI. ANALISI DE COMPLIMENT INICIAL.

En primer lloc hem realitzat un anàlisi del estat de compliment inicial dels controls del Annex A de la norma 27001.

A.5 Polítiques de Seguretat de la Informació
A.6 Organització de la seguretat de la informació
A.7 Seguretat relativa als recursos humans.
A.8. Gestió d'Actius
A.9 Control d'accés.
A.10. Criptografia.
A.11 Seguretat Física i del Entorn
A.12 Seguretat de les operacions.
A.13 Seguretat de les comunicacions.
A.14 Adquisició, desenvolupament i manteniment dels sistemes de la informació.
A.15 Relació amb els proveïdors.
A.16 Gestió dels incidents de Seguretat de la informació.
A.17. Aspectes de Seguretat de la informació per a la gestió de la continuïtat del negoci.
A.18 Compliment.

Hem Avaluat Per cadascun dels controls de la norma l'estat inicial de la organització vers aquest amb la taula del Excel inclòs al Annex del present document. Per altre banda el mateix document ens servirà de document d'Aplicabilitat de controls o SOA del SGSI.

Per un costat hem definit el control:

ISO 27001:2013 Controls			
Sección	Control		
Políticas de seguridad de la información	5.1	Directrices de gestión de la seguridad de la información	Objetivo: Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas
	5.1.1	Políticas para la seguridad de la información	Control Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
	5.1.2	Revisión de la política de seguridad de la información	Control Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Per altre:

- L'Aplicabilitat del mateix.
- El grau de maduresa (Inexistent, Inicial, Reproduïble, Definit, Mesurable, Optimitzat)
- Em implantat un valor quantificable, del grau d'implantació, que creiem un possible valor de millora i granularitat vers l'indicador
- I hem obtingut d'aquests càlculs uns valors estimats inicials que mostrarem a continuació en les diferents taules.

Així per tant si el control Aplica

- Marcarem la columna Aplicable
- I l'estat es Optimitzat (grau mes alt de maduresa)
- Valor del grau d'implantació 5 (valor mes alt)
- I es repeteix per tots els Controls de la secció. Obtindríem que el total de la secció es 10 que implicaria un 100%.

Ho mostrarem al següent exemple.

Aplicable	Inicial	Reproduïble	Definit	Mesurable	Optimitzat	Valor grau d'implantacio	Total
	Marcar x	Marcar x	Marcar x	Marcar x	Marcar x	Valorar de 1 a 5	
Applicable	x	x	X	X	X	5	
	1,00	1,00	1,00	1,00	1,00	5,00	10,00
Applicable	x	X	X	X	X	5	
	1,00	1,00	1,00	1,00	1,00	5,00	10,00
					Total objetivo 5.1		**20,00**
					Total sección 5		**10,00**

Un cop aplicades aquestes valoracions inicials als diferents controls de la normal ISO/UNE 27001:2013, que podem veure detallats a la taula Annexa al present document, "*Annex A.- SOA - Anàlisis diferencial TFM.xlsx* "

Obtenim la següent taula de resultats:

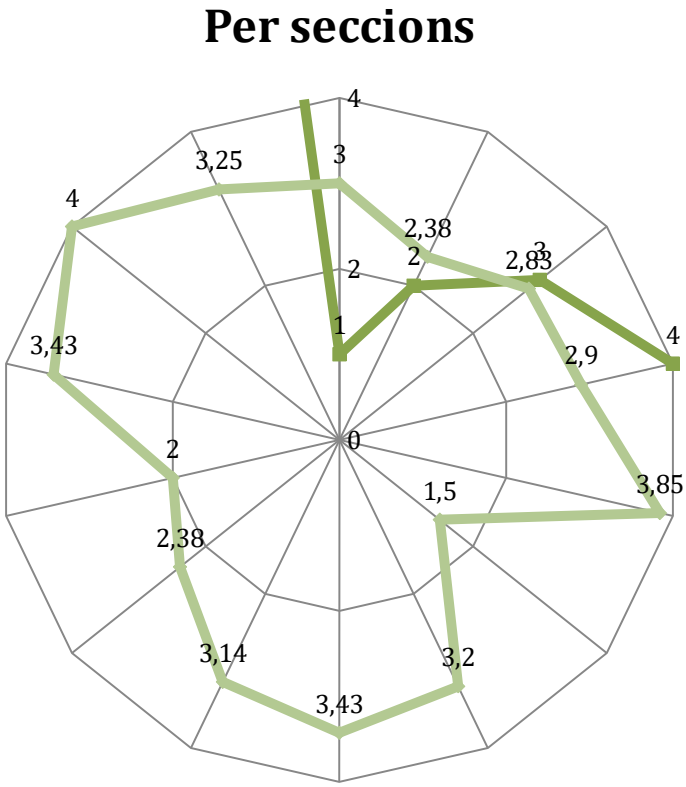
5. Políticas de seguridad de la información	**Total sección 5**	**3,00**
6. Organización de la seguridad de la informació	**Total sección 6**	**2,38**
7. Seguridad relativa a los recursos humanos	**Total sección 7**	**2,83**
8. Clasificación de la información	**Total sección 8**	**2,90**
9. Control de 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**

Del que podem avaluar que el total inicial definit del nostre Sistema es de 2,95 punts.

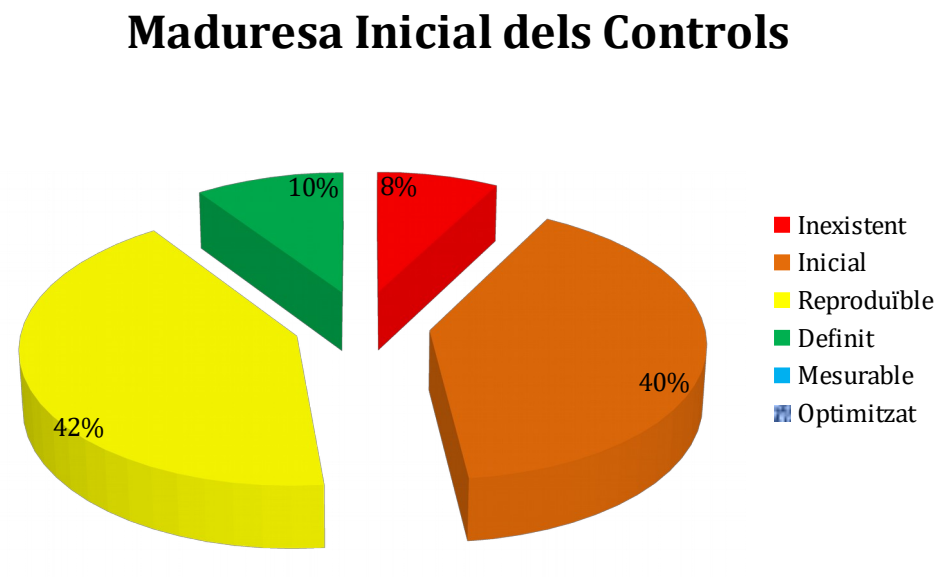
Destacarem que en una primera instància i revisio´ del estat inicial tots els controls aplicarien al nostre sistema excepte el control 11.1.6 Referents a Àrees de Carrega i descarrega. Ja que no existeixen a la organització del present exercici.

11.1.6	Áreas de carga y descarga	Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.	No Applicable

De les mateixes dades podem obtenir un diagrama de radar tal i com ens indica l'enunciat d ela fase1 dels apunts de l'assignatura:



En quant al estat de Maduresa Inicial dels controls podem veure un quadre representatiu que mostrarem a continuació.



Les dades del mateix les referirem en la següent taula, que podem trobar al Full2 del "*Annex A.- SOA - Anàlisis diferencial TFM.xlsx* "

Inicial	46
Reproduïble	48
Definit	11
Mesurable	0
Optimitzat	0

Observem que la majoria de controls es troben en un estat Reproduïble però intuïtiu, que recordarem que és defineix com, que "Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca, es normalitzen les "bones pràctiques" en base a l'experiència i al mètode.

OBJECTIUS A ASSOLIR.

En una primera instància l'objectiu que tenim a assolir es tractar treballar i madurar els processos de control. Així doncs tractarem d'evolucionar aquests.

- De Inicial almenys a Reproduïble
- De Reproduïble a Definits

Per assolir aquests objectius implementarem el següent SGSI emprant un sistema de treball de millora continua o PDCA (Plan Do Check Act)

4. FASE 2. COS DOCUMENTAL.

En aquesta segona fase del projecte tractarem i desenvoluparem el cos documental per al compliment normatiu del SGSI.
Aquests documents venen establerts a la normativa vigent ISO/IEC 27001:2013.

L'índex o esquema en el que ens centrarem en aquesta Fase 2 vindrà determinat a les especificacions del TFM.

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

Posteriorment i com a opció de Millora proposat al Tutor desenvoluparem l'estudi d'un projecte d'unificació de Sistemes de Gestió, Aquest document de proposta d'Ampliació el trobarem durant tot el desenvolupament del projecte en les últimes pàgines del mateix.

4.1. POLÍTICA 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.

La nostra política de Seguretat es basarà en els següents pilars bàsics que mes endavant desenvolupament mes acuradament:

BASES DE LA POLITICA DE SEGURETAT DE MUTUA INTERUNIVERSITARIA.

Crearem un resum de les Bases de la Política de Seguretat per tal de fer arribar a tothom la idea del concepte i per tal de que ells puguin aprofundir en quin es el contingut del mateix llegint posteriorment la Política de Seguretat.

- 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-la i mantenir-la a 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

POLITICA DE SEGURETAT DE MUTUA INTERUNIVERSITARIA.

Podem trobar el document referent a la Política de Seguretat de la Mutua Interuniversitària adjunt al present document a l'Annex G. Política de Seguretat.

4.2. PROCEDIMENTS D'AUDITORIES INTERNES.

El Procediment d'Auditoria Interna fa Referència al Apartat 9.2 de la ISO/IEC 27001:2014.
L'objectiu d'aquest procediment es establir i descriure com es porten a terme les auditories Internes del Sistema de Gestió de la Seguretat de la Informació, com es registren les desviacions, com son acordades, complimentades i verificades les accions correctives i preventives apropiades.
El resultat de les auditories deu ser tal que permeti comprovar si l'SGSI.

- Es conforme amb la política de seguretat, amb les especificacions d'aquesta norma i amb els requisits establerts per la Organització.
- S'ha implantat, es manté i s'executa de forma eficaç
- El procés d'auditoria és adequat per la gestió dels actius, les amenaces i els riscos. i el seu valor, així com les amenaces i riscos de la Organització.
- Verificar els registres de revisió de la anàlisis de riscos.

ABAST DE LES AUDITORIES INTERNES
L'abast de les auditories internes es igual que l'abast de tot el SGSI de la Organització. Afectaran a tota la Organització

REGISTRES
Els registres que deriven d'aquest procediment es guardaran com a documentació d'auditoria i s'empraran per realitzar el posterior informe d'auditoria periòdic i l'informe final d'auditoria Interna.

RESPONSABILITAT
Les auditories Internes del SGSI son portades a terme pel Responsable de Seguretat o per qualsevol altre membre del equip d'auditors qualificats. L'auditor designat ho serà amb la condició de que no tingui responsabilitats directes en l'àrea de treball o departament que serà auditat. L'auditor intern ha de tenir una formació prèvia en auditoria Interna. (Revisar cursos de Formació per perfil)

PERIODICITAT.
Les auditories Internes del SGSI es realitzaran periòdicament, encara que com a mínim s'efectuarà una auditoria integral cada any.

PLÀ D'AUDITORIA.
Els Plans d'auditoria realitzats s'arxivaran en la BBDD del SGSI, a l'apartat de Documents.
El pla d'auditoria serà establert pel Responsable de Seguretat o per qui ell designi, notificant amb un temps prudencial d'antelació a la primera auditoria programada. Quan es defineixi el calendari d'auditories o modificacions sobre aquest el Responsable de Seguretat enviarà un marcador al equip d'auditors i als Responsables dels departaments implicats pel seu coneixement. S'establirà l'abast de l'auditoria definint els processos que s'auditaran.
Els criteris de cada auditoria els triarà el cap d'auditors en funció del seu coneixement del SGSI.

A mes de les auditories programades, es podran concertar auditories ocasionals, sota la supervisio´ del Responsable de Seguretat, en resposta a una situacio´ insatisfactòria o increment considerable d'incidències de Seguretat.
La direcció podrà definir auditories no programades en aquells casos en que ho consideri necessari, prèvia notificació per escrit.

EQUIP D'AUDITORS INTERNS
Per tal de realitzar les auditories internes es mantindra` format a un equip d'auditors Interns. La formació serà implantada pel responsable de Seguretat o la persona que aquest designi a tal efecte. La capacitat del formador d'auditors estarà avalada pel Responsable de Seguretat i pels cursos que a tal efecte hagi realitzat el formador.
FASES I EXECUCIÓ DE L'AUDITORIA

Les auditories internes del SGSI es realitzaran seguint les següents fases:

- Preparacio´ de l'auditoria. L'auditor prepararà una taula amb els punts a auditar, seguint el format establert en la norma, per tal de ser emprada a l'auditoria en la que haurà de tenir en compte, procediments, controls, objectius o altre documentació rellevant del departament. Aixı´ com desviacions fruit d'auditories anteriors. L'auditoria de cada activitat o departament la realitzara` un auditor alie` a la esmentada activitat per evitar duplicitat de funcions.
- **Notificació de l'auditoria.** L'Auditor haurà de notificar qualsevol auditoria que pretengui realitzar als caps de departament responsables de les àrees a auditar amb un temps prudencial d'antelació, per tal de concertar un termini i un horari adequat per realitzar-la.
- **Reunió Preliminar**. L'auditor i els caps de departament tindran una reunió preliminar on es confirmarà l'àmbit de l'auditoria, el programa i tot el referent a desviacions i accions correctores
- **El procés d'auditoria.** Durant el procés d'auditoria, l'auditor haura` d'estar acompanyat, preferiblement, d'un representant del àrea que estigui sent auditada. Quan l'auditor detecti una deficiència la comentarà amb el responsable del àrea en qüestió, arribant a un acord sobre la evidència dels fets observats. S'haurà d'anotar les evidencies o els exemples que demostrin la desviació. Tanmateix es comentaran i anotaran les possibles millores i punts forts detectats.
- **Durant el procés d'auditoria.** Es verificaran els controls, el seu grau d'implantació i la seva eficàcia. A mesura que es vagin auditant els punts de la norma es registraran en el formulari.
- **Informe sobre l'auditoria Interna.** Un cop finalitzada l'auditoria, l'auditor cap recollirà les taules de punts auditats amb les possibles notes de desviació i realitzarà un informe resumint-les totes, identificant clarament el departament auditat, la data d'auditoria i detallant els següents punts.
    - Detalls de les desviacions, millores, indicant, el títol, número i documents als que es refereix.
    - Lloc on s'ha detectat la desviació o millora o punt fort
    - Detalls de les accions correctores/preventives, acordades i data en la que hauran de ser corregides. Aquestes derivades de l'auditoria interna, seran tramitades tal i com s'especifica en el procediment de Accions correctives i Preventives.

- Aquest informe d'auditoria serà afegit al sistema documental del SGSI i arxivat a l'apartat de Documents.
- Per altre banda es disposarà d'un arxiu en paper on es recolliran les notes de desviació que pertanyin a l'auditoria i les taules dels punts auditats. Aquest arxiu estarà sota la responsabilitat del Responsable de Seguretat.

- **Seguiment i tancament de l'auditoria Interna.** Totes les possibles accions correctives/preventives derivades de l'auditoria interna hauran de ser supervisades pel cap d'auditoria, no considerant-se la auditoria interna com a tancada fins que totes aquestes estiguin tancades.

5. GESTIÓ D'INDICADORS.

OBJECTIU
La ISO/IEC 27001:2005 va introduir un nou concepte a la SGSI, es tractava del indicador de l'eficàcia dels controls, que permetia al SGSI avaluar la eficàcia i la qualitat del mateix.

En la ISO/IEC 27001:2013 es parla de la mesura i avaluació del sistema en el seu punt 9.1

La gestió dels indicadors es una de les línies de la Millora continua del sistema, això es degut a la natura d'aquests ja que durant el disseny de cada control es seleccionaran una sèrie d'indicadors que s'empraran per avaluar l'eficàcia del control un cop implantat.

Avaluant la eficàcia dels controls podrem avaluar també la eficàcia del valor que aporta a la companyia mesurar els controls i ens permetrà portar a terme el PDCA sobre el SGSI.

Aquests indicadors es definiran sempre que sigui possible i que les evidencies siguin fiables, objectives i rellevants.

PERIODICITAT
Durant el cicle de vida del SGSI es revisaran anualment els indicadors, això permetrà avaluar l'eficàcia dels mateixos i la necessitat d'incloure o excloure'n.

DOCUMENTACIÓ I GUIES.
Podem trobar documentació sobre la implantació de Mètriques e indicadors en diferents fonts, per la nostra implantació emprarem per un costat la documentació de mètriques e indicadors del ENS (Esquema nacional de seguretat)

6. PROCEDIMENT DE REVISIÓ PER LA DIRECCIÓ

OBJECTIU
Correspondria al apartat 9.3 de la UNE-ISO 27001:2014. En aquesta assentarem les bases de la Revisió del Sistema de Gestió de Seguretat de la Informació per la direcció.

PERFILS AFECTATS
Responsable de Seguretat, Comitè de Gestió de Seguretat de la Informació, Direcció General.

DESENVOLUPAMENT
Per implementar la Revisio´ del Sistema per la direccio´ es realitzaran els següents procediments.

- En primer lloc es revisarà la política de seguretat.
  - Ha d'esser difosa a la organització mitjançant la formació inicial als empleats i la seva publicació en el portal corporatiu de la Organització.
  - També s'ha publicat un document de política abreviada, un document de les responsabilitats del personal i a la part publica del document de Seguretat de la L.O.P.D
  - Per assegurar que el personal recorda i coneix la política de Seguretat i les seves responsabilitats, la organitzacio´ establira` un Objectiu amb accions trimestrals de seguiment.
- Revisió dels resultats dels Anàlisis de Riscos.
  - S'extreu un resum de les conclusions dels anàlisis de Riscos respecte a les dimensions de Disponibilitat, Confidencialitat e Integritat.
- Identificació de noves vulnerabilitats i amenaces
  - S'identifiquen les possibles noves vulnerabilitats i amenaces detectades en quant a:
    - Seguretat Física
    - Seguretat Lògica
    - Seguretat en BBDD
    - Seguretat en Internet
    - Seguretat Ofimàtica
    - Seguretat
- Es revisen les Incidències de Seguretat.
  - Revisió del estat de les incidències mes importants
- Seguiment dels indicadors del SGSI
  - Revisió del estat dels indicadors mes significatius.
- Resultats de les Auditories de Seguretat
  - Auditories Internes
  - Auditoria Biennal LOPD
  - Auditoria Externa o de certificació
- Propostes per part del personal.
- Revisió de les Necessitats de Formació en Seguretat.
  - Es revisa l'estat de Maduresa del personal de la organització i es proposen noves iniciatives i cursos per portar a terme en termes de seguretat.

- Accions de Millora
    - Es revisa la base de dades per la gestió de les accions de millora
- Revisió del Informe de Revisió Anterior
- Revisió i Seguiment dels Objectius
- Conclusions.
    - Del estat del Sistema
    - Objectius a curt i mig termini

Aprovació i continuïtat del Sistema per part de direcció

7. GESTIÓ DE ROLS I RESPONSABILITATS

OBJECTIU
En el punt 5.3 de la ISO 27001:2014 se'ns fa referència a Rols, Responsabilitats i autoritats en la organització.

Així doncs totes les responsabilitats en seguretat de la informació han d'estar definides i assignades, aquest procediment te com a Objectiu definir les responsabilitats sobre seguretat de la informació.

ABAST.
La gestió dels Rols i les responsabilitats afectarà a tota la Organització.

PERFILS AFECTATS
Definits en el propi document.

RESPONSABILITATS SOBRE ELS ACTIUS.
Les responsabilitats sobre els actius individuals quedaran reflectides en les següents taules, cada responsable es propietari del actiu. Les responsabilitats que s'atribueixen a cada propietari son:

- Velar juntament amb el Responsable de Seguretat pel compliment de tots aquells aspectes reflectits en la documentació del SGSI
- Velar per tal de que tot el personal assignat al seu càrrec conegui i apliqui els procediments pertinents.
- Velar per tal de que tot el personal al seu càrrec comuniqui de forma ràpida, clara i concisa qualsevol incidència de seguretat.
- Avaluar aquells controls que tingui al seu càrrec, suggerint al SGSI qualsevol millora del sistema.
- Mantenir els registres que estiguin sota la seva responsabilitat de forma correcta.

ACTIUS FISIC I DE NEGOCI. Les responsabilitats per als actius individuals queden reflectides de la següent manera. Cada responsable es propietari del actiu.

ACTIUS FISICS i DE NEGOCI	RESPONSABLE
Aplicacions de Gestió Administrativa	Director de RRHH
Aplicació Història Clínica	Director de AT
Aplicacions del Sistema de Gestió	Director de T.I.
Aplicacions d'Usuaris	Director de T.I.
Aplicacions de Correu Electrònic	Director de T.I.
Aplicacions de Gestió de RRHH	Director de RRHH
Aplicacions de Direcció	Director de T.I.

EQUIPS INFORMÀTICS	RESPONSABLE
Sistema Storage SAN	Director de T.I.
Servidores Crítics	Director de T.I.
Servidores no crítics	Director de T.I.
Sistemas de Backup	Director de T.I
Connectivitat y comunicacions	Director de T.I
Estaciones de Trabajo e impressió	Director de T.I

LOCALS	RESPONSABLE
CENTRES ADMINISTRATIUS	Director d'Enginyeria
DISPENSARIS	Director d'Enginyeria

ENTORN	RESPONSABLE
SUMINISTRAMENT ELECTRIC	Director d'Enginyeria
NETEJA	Director d'RRHH
CLIMATITZACIÓ	Directora de Qualitat i Medi Ambient

PERSONAL	RESPONSABLE
PERSONAL SANITARI	Director d'RRHH
DIRECTORS EXECUTIUS	Director d'RRHH
DIRECTORS FUNCIONALS	Director d'RRHH
PERSONAL ADMINISTRATIU	Director d'RRHH

ALTRES	RESPONSABLE
CONFIANÇA DELS CLIENTS	Director de Client Extern
IMATGE DE MARCA	Director de Marketing

DADES	RESPONSABLE
DADES DE GESTIÓ ADMINISTRATIVA	Director de RRHH
DADES D'HISTORIA CLÍNICA	Director Mèdic
DADES D'USUARIS	Director de RRHH
DADES DE CORREU ELECTRONIC	Director de T.I

DADES DE GESTIÓ DE RRHH	Director de T.I
DADES DE DIRECCIÓ	Director General

SERVEIS	RESPONSABLE
INFRAESTRUCTURES	Responsable de Sistemes
APLICACIÓNS T.I	Director de T.I
PROJECTES	Oficina de Projectes
SERVEIS JURIDICS	Director de RRHH
SEGURETAT FÍSICA	Responsable de Seguretat
QUALITAT I MEDI AMBIENT	Responsable de Qualitat i Medi Ambient
FORMACIÓ DE SEGURETAT	Responsable de Seguretat

RESPONSABILITATS SOBRE PROCESSOS ESPECÍFICS (OPERACIONALS)

Tots els procediments operacionals tenen com a responsable i propietari al Responsable de Seguretat, excepte aquells que específicament indiquin els directors de RRHH i Director de Client Intern sobre els quals assumeixen responsabilitat pròpia per exemple.

- Procediments d'autenticació, identificació i auditoria
- Procediments d'alta i baixa d'usuaris
- Procediments d'autorització d'altes de nous recursos
- Procediments d'autorització

Aquests es trobarien sota la responsabilitat del director.

DELEGACIÓ.

Els propietaris dels actius de la informació poden delegar les seves responsabilitats de seguretat en directius a títol individual o en proveïdors de serveis, tot i això el propietari continuarà tenint la responsabilitat final sobre la seguretat del actiu i ha d'estar capacitat per a determinar que qualsevol delegacio´ de responsabilitat s'ha portat a terme correctament.

IDENTIFICACIÓ D'ACTIUS I PROCESSOS PER SISTEMA.

Actualment el procés de definició de processos es troba en pla de desenvolupament. El responsable dels actius es actualment el responsable del procés.

NIVELL D'AUTORITZACIÓ.

La única persona que podrà autoritzar processos específics o canvis dels processos se Seguretat és el Responsable de Seguretat, ja que es l'encarregat de validar qualsevol acció que pugui afectar a aquesta.

Els director de RRHH aportaran al Comitè de Seguretat les propostes de canvi i aquestes seran aprovades per aquest organisme i portades a terme per les persones designades pel mateix.

OBLIGACIONS I RESPONSABILITATS DEL PERSONAL.

La Organització disposa d'un document d'Obligacions i Responsabilitats del personal, que es subministrat també a tercers vinculat als requisits legals de la LOPD, que s'ha extrapolat a la resta de dades propietat de la Organització, aquest document està a disposició de tots els empleats a la Intranet de la Organització.

Les funcions i Responsabilitats sobre la Seguretat de la Informació, d'acord amb la política de Seguretat de la Organització es documenten en la política de Seguretat, en els perfils dels llocs de treball i en el procediment de control, tant mateix es realitza l'assignació de responsabilitats de seguretat de la informació en la taula de propietari dels actius, així com en els procediments inclosos en el sistema de gestió.

Aquestes funcions i responsabilitats inclouen, la responsabilitat general per implantar o mantenir la política de seguretat, així com qualsevol responsabilitat específica per a la protecció d'actius particulars, la execució dels processos o activitats particulars de seguretat, la garantia de que la responsabilitat de les accions realitzades es assignada a individus i la informació d'esdeveniments o possibles esdeveniments de seguretat o altres riscos de seguretat per a la Organització.

Aquestes responsabilitats son plasmades de forma contractual en aquells aspectes exigits per la legislació vigent en interès de la Organització, juntament amb aquells no legalment exigibles però considerats necessaris per la Organització inclosos els cursos de Formació inicials i Posteriors

METODOLOGIA I ANALISIS DE RISCOS.

Descriurem a continuació la metodologia, criteris o operació emprats pel desenvolupament de la Anàlisi de Riscos de la Organització. Trobarem referencies al tractament dels riscos i al pla de gestió del Risc al punt 8.2 i 8.3 de la ISO/IEC 27001:2013, tot i que també ens guiarem per la Normativa ISO 31000:2009 sobre la gestió del Risc.

8.1. ABAST.

Aquest procediment afectarà a tots els actius relacionats amb l'abast del SGSI.

8.2. PERFILS AFECTATS.

Els perfils afectats seran la direcció, El Responsable de Seguretat i El Comitè de Gestió de la Seguretat.

8.3. DESENVOLUPAMENT.

La organització pretén elaborar un procediment d'anàlisis de riscos, per tal tasca aquesta es recolzarà en una metodologia d'anàlisis de Riscos coneguda com Magerit, per gestionar aquests, tot i que n'existeixen d'altres com per exemple COBIT, Octave.(podem veure també comparatives d'aquestes en els documents mencionats en la bibliografia adjunta).

És pretén implementar una valoració dels actius i dels riscos als que aquests estan exposats. Per tal d'implementar la valoració del risc haurem d'identificar les amenaces que poden comprometre aquests actius, la seva vulnerabilitat i l'impacte d'aquests a la Organització que procedirem a quantificar determinant el nivell de risc. Per portar-ho a terme Les fases que implementarem seran les següents:

- Estudi previ sobre els Actius
- Valoració i Marc referencial
- Identificació, del grup d'Actius i valoració en funció de la seva Dimensió
- Identificació de les Amenaces Aplicables al Anàlisis de Riscos
- Procés de Valoració i obtenció de Resultats.
- Gestió del Anàlisis de Riscos i Evolució Continua del Mateix.

8.3.1. ESTUDI PREVI SOBRE ELS ACTIUS.

Amb el fi d'abordar un anàlisis de Riscos alineat completament als interessos de la Organització i als seus plans estratègics s'ha realitzat un estudi dels Actius claus de negoci, i s'ha relaciona cada un dels actius físics, immaterials, de persones. Etc. a cada actiu de negoci, agrupant-los en funció del seu gènere i valor per a la organització .

8.3.2. VALORACIÓ I MARC REFERENCIAL.

La Organització crea unes taules de valoració dels actius, amb valors discrets dels valor dels actius, de valoració de la freqüència en la que pot donar-se una amenaça i del impacte que aquesta pot produir, dels criteris en que un determinat tipus de salvaguarda podrà disminuir la freqüència o l'impacte d'una amenaça i determina el significat dels següents termes dins del anàlisis de riscos.

- Risc Intrínsec: Es aquell que pateix un actiu davant d'una amenaça sense aplicar cap salvaguarda.
- Risc Efectiu: Es el que pateix un actiu davant d'una amenaça un cop aplicades les salvaguardes que li afecten.
- Risc Residual: És el risc que la Organització ha establert com a risc assumible per la mateixa i recolzat per la direcció.
- Salvaguarda: Aplicació de un % determinat per l'autor del Anàlisis de Riscos dels controls que afecten a un determinat objectiu amb el fi de protegir l'actiu.

Les Taules de Criteris de valoració es descriuen en la primera fulla de cada anàlisis per dimensió

8.3.3. IDENTIFICACIÓ DELS ACTIUS I VALORACIÓ EN FUNCIÓ DE LA SEVA DIMENSIÓ..

Un cop agrupats els actius, es procedeix a la seva valoració per a cada una de les dimensions contemplades a la anàlisis, tractarem en primera instància Disponibilitat Confidencialitat e Integritat, generant tres fulls d'anàlisis diferents en funció de cada dimensió tractada.

8.3.4. IDENTIFICACIÓ DE LES AMENACES APLICABLES AL ANALISIS DE RISCOS.

La Organització ha seleccionat les amenaces que poden afectar als actius considerant-les tal qual o agrupant-les en aquells casos en que les ha considerat que eren equivalents, consensuant-les amb el comitè de direcció. Ho ha detallat a la fulla de càlcul que mostrarem a l'exemple. Per implementar-ho ens hem documentat entre altres en la guia Magerit, ISO 27005:2008 (Risk Management), I en un curs de Gestió de Riscos de T.I, documentat en la bibliografia adjunta al present document.

8.3.5. PROCES DE VALORACIÓ I OBTENCIÓ DE RESULTATS..

El procés de valoració del anàlisis de Riscos es el següent:

- Per a cada actiu i respecte de cada una de les amenaces es determina si afecta o no al actiu.
- La Freqüència en la que pot donar-se la amenaça
- L'impacte de l'amenaça pot tenir sobre l'actiu.

El sistema calcula en funció d'aquests paràmetres un valor de Risc Determinat.

El sistema agruparà els riscos sobre els actius per cadascuna de les amenaces.
Un cop obtingut el risc Intrínsec, es procedeix a valorar quines salvaguardes (agrupades per objectius de control) ha adoptat la Organització respecte a cada amenaça, valorant:

- en quin grau disminueixen la vulnerabilitat (preventivament)
- O l'impacte si es produeix la amenaça respecte l'actiu.

Després de la valoració del grau d'implantació de les salvaguardes es possible obtenir:

- el resultat del risc efectiu sobre cada un dels actius
- la disminucio´ del risc obtinguda gràcies a la aplicacio´ de les salvaguardes pertinents.

El Risc efectiu s'agrupa i tracta per cada amenaça per tal de poder comparar aquest risc amb el risc que la Organització ha acceptat com a risc Residual Acceptable.

Al final del procés de càlcul es possible apreciar:

- gràfics de la distribució del valor dels actius
- De la disminució del Risc obtinguda per les salvaguardes
- Del valor del Risc Efectiu.

A partir dels resultats es possible valorar aquelles amenaces i actius que requereixen l'aplicació de salvaguardes addicionals que permeten portar el nivell de risc efectiu a un nivell per sota del llindar assumible per la organització i fruit d'això activar noves mesures i projectes de millora. Així com activitats correctives i preventives.

El sistema permet la avaluació dels costos de les salvaguardes aplicades de forma genèrica, així com poder obtenir certa aproximació a les necessitats de inversió de cada a aplicar les noves salvaguardes.

Ho desenvoluparem a la FASE 3 del present document. I Adjuntarem els diferents anàlisis de riscos en els Annexos adjunts, per les diferents Dimensions del risc, Disponibilitat, Confidencialitat e Integritat. Annexos D,E,F, respectivament.

8.3.6. GESTIO DEL ANÀLISIS DE RISCOS I EVOLUCIÓ CONTINUA DEL MATEIX..

Factors que intervindran en la modificació i evolució del anàlisis de riscos.

CONSTANTS.
Els valors dels actius es mantindran constants al llarg del temps així com els criteris de valoració discrets, això donarà peu a tenir un marc de referència estable amb el fi de que les comparacions amb el marc inicial permetin veure la correcta evolució del sistema.

VARIABLES.

- La valoració de la periodicitat en la que pugui donar-se una amenaça serà un factor molt important a valorar i que s'haurà de modificar al percebre aquest fet, ja sigui per incidències repetitives, mesures de control deficients. Etc

- El grau d'impacte que produeix una amenaça haurà també de considerar-se davant d'una incidència de seguretat i valorar-se respecte a l'experiència adquirida en el succés.
- S'haurà de revisar el grau d'aplicació de les salvaguardes i la seva influencia en la protecció dels actius, això implica la avaluació continua dels controls mitjançant la mesura dels mateixos i comparar-ho amb els resultats obtinguts gràcies a la seva aplicació. Per exemple la reducció d'incidències que afectin a aquest actiu.
- Durant els processos de revisió del sistema es valorarà la inclusió de noves amenaces al anàlisis de riscos, ja sigui fruit de la informació aportada per les incidències o aportació de informació addicional que el comitè de gestió estimi oportuna

9. DECLARACIÓ D'APLICABILITAT

SELECCIÓ DE CONTROLS SOA

La relació de controls a Implantar, s'han seleccionat entre els descrits en els enunciats dels punts de la norma ISO/IEC 27002:2015 de bones pràctiques vigent. Seguint la normativa ISO/IEC 27001:2014 on en el seu apartat 6.1.3 ens parla del Tractament dels Riscos de Seguretat de la Informacio´ i concretament en el 6.1.3.d on ens indica elaborar una declaracio´ d'aplicabilitat que contingui els controls necessaris i la justificacio´ de les inclusions i exclusions dels mateixos.

Així doncs es mantindrà actualitzada la versió de la norma 27002:2015 per tal d'estudiar la inclusió de nous controls.

SI un o diferents controls de la norma ISO/IEC 27002:2015 no es poden aplicar degut a la natura de la Organització i la seva activitat es considerarà la seva exclusió.

Les exclusions dels controls es fonamenten en el resultat del anàlisis de Riscos de la Organització i de l'aplicabilitat dels mateixos a la Organització.

Destacarem que en una primera instància i revisio´ del estat inicial tots els controls aplicarien al nostre sistema excepte el control 11.1.6 Referents a Àrees de Carrega i descarrega. Ja que no existeixen a la organització del present exercici.

Podem veure el SOA inicial juntament amb la Anàlisis diferencial desenvolupat fins el moment en el document adjunt.

"Annex A.- SOA - Anàlisis diferencial TFM.xlsx "

10. FASE 3. GESTIÓ DEL RISC

En aquesta fase haureu de fer una identificació i valoració del actius i amenaces a les que està sotmesa l'organització, pretendrem respondre a les preguntes:

- Quins actius Importants té l'organització?
- Quin és el seu valor?
- Farem una Avaluació i quantificació d'amenaces
- Finalment Avaluarem el Risc Potencial i del impacte.

Per portar-ho a Terme ens basarem en les Següents Sub fases.

- 10.1- ANALISI DELS ACTIUS RELLEVANTS DE SEGURETAT – ESTUDI PREVI SOBRE ELS ACTIUS.
- 10.2- ESTUDI DE LES POSSIBLES AMENACES E IMPACTE SOBRE ELS SISTEMES D'INFORMACIÓ.
- 10.3- AVALUACIÓ DEL RISC E IMPACTE POTENCIAL SOBRE ELS ACTIUS

Cadascuna d'aquestes sub fases tindra` a la vegada diferents punts de desclòs que conformaran la anàlisis, classificacio´ i determinacio´ final de la sub fase, seguint la metodologia Magerit d'anàlisis de Riscos.

10.1. ANALISI DELS ACTIUS RELLEVANTS DE SEGURETAT – ESTUDI PREVI SOBRE ELS ACTIUS.

OBJECTIUS:
Els actius associats a la informació i als recursos per el tractament de la informació han d'estar clarament identificats i han d'elaborar-se i mantenir-se en un inventari.

ROLS INVOLUCRATS.
Direcció
Responsable de Seguretat
Responsable d'Infraestructures
Director Financer
Auditor Intern

ABAST:
Tota la Organització.

DESENVOLUPAMENT:
La organització posseeix un inventari d'actius com a base per aconseguir una protecció eficaç dels mateixos, aplicant les mesures adequades, Aquesta serà la base del anàlisis de Riscos.
Per raons de protecció laboral, cobertures de pòlisses d'assegurança adequades i per motius de control financer, amortitzacions, etc..
En aquest inventari es reflecteix el valor e importància relatius a cada un dels actius i s'implementara` la valoracio´ dels mateixos per proporcionar nivells de protecció proporcionals al valor e importància d'aquests.

Existeix també en el esmentat inventari d'actius rellevants l'associació o relació amb cada sistema d'informació o procés de negoci, identificant clarament, la classificació de seguretat i la situació habitual.

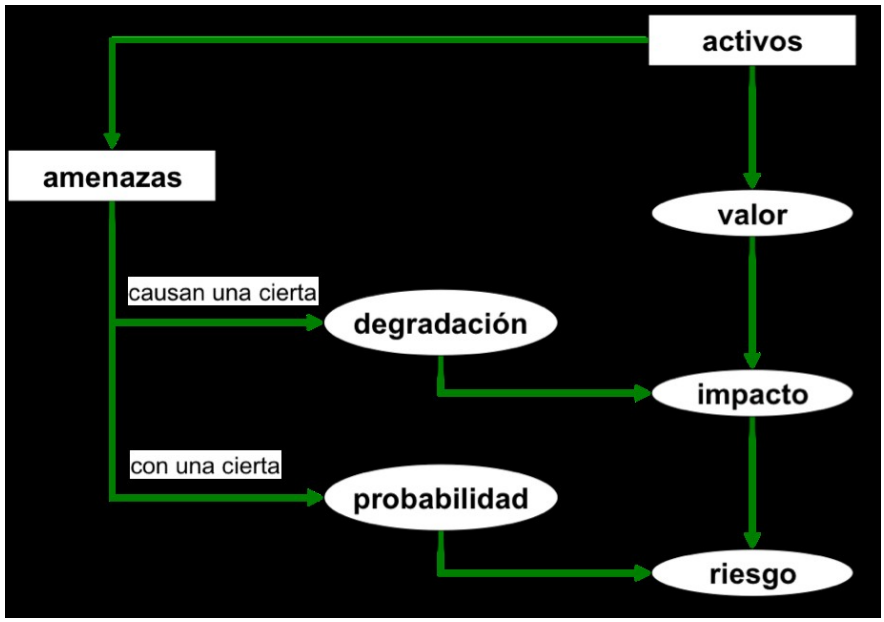
Tal i com hem comentat aplicarem la metodologia Magerit que en grans termes es defineix a continuació.

MAGERIT

La anàlisis de riscos es una aproximació metòdica per determinar el risc seguint uns passos pautats:

1. Determinar els actius rellevants per a la Organització, la seva interrelació i el seu valor, en el sentit de quin cost suposa la seva degradació.
2. Determinar a quines amenaces estan exposats aquells actius
3. Determinar quines salvaguardes hi ha disposades i com d'eficaces son davant del risc.
4. Estimar l'impacte, definit com el dany sobre l'actiu derivat de la materialització de l'amenaça
5. Estimar el risc, definit com l'impacte ponderat amb la tassa d'ocurrència, o expectativa de materialització de la amenaça.

Amb l'objecte d'organitzar la presentació s'introdueixen els conceptes d'impacte i Risc "potencials", entre els passos 2 i 3. Aquestes valoracions son "Teòriques" en el cas de que no hi hagués salvaguarda encara desplegada. Un cop obtingut aquest escenari teòric, s'incorporen les salvaguardes del pas 3, derivant estimacions realistes d'impacte i de risc. La següent figura recull aquest primer recorregut.



Nosaltres estendrem una mica mes aquest esquema per tal de poder:

- Definirem els Tipus dels actius, sub tipus i serveis associats

- Estipularem una taula de valoració dels actius
- Classificarem els actius per Tipus i procés de Negoci definit a l'Abast
- Valorar els actius per les dimensions de Confidencialitat, Disponibilitat, e Integritat.
- Determinar les amenaces
- Determinar l'impacte de les amenaces sobre els diferents els actius
- Determinar com disminueixen el risc les salvaguardes sobre les amenaces
- Estimar el Risc.

10.2. ANÁLISI FUNCIONAL GESTIÓ DEL RISC.

A l'Annex H. Anàlisi Funcional de Gestió del Risc implementarem tot l'anàlisi funcional i els diferents aspectes implicats en la Gestió del Risc de la Mutua Interuniversitària.

Dins d'aquest Annex desenvoluparem de forma detallada els següents Aspectes del Anàlisi de Risc.

- TAULA D'ACTIUS
- TAULA DE VALORACIÓ
- TAULA DE VALORACIÓ D'ACTIUS
  - DIMENSIO CONFIDENCIALITAT
  - DIMENSIÓ D'INTEGRITAT
  - DIMENSIÓ DISPONIBILITAT
- ESTUDI DE LES POSSIBLES AMENACES E IMPACTE SOBRE ELS SISTEMES D'INFORMACIÓ
  - TIPOLOGIA FONTS D'AMENACES
  - TIPUS I SUBTIPUS D'AMENACES
- AVALUACIÓ DEL RISC E IMPACTE POTENCIAL SOBRE ELS ACTIUS
- DEFINICIÓ DE SALVAGUARDES.
  - TAULA DE SALVAGUARDES
  - EVALUACIÓ SALVAGUARDA AMENAÇA
- CALCUL DEL RISC EFECTIU.

Referenciarem també els diferents Annexos referents a les taules de càlcul del risc que puntejarem també a continuació.

- Anàlisis i avaluació del Risc de Confidencialitat (Annex D -Risc Confidencialidad.xls)
- Anàlisis i avaluació del Risc de Risc Disponibilitat(Annex E -Risc Disponibilitat.xls)
- Anàlisis i avaluació del Risc de Risc d'Integritat (Annex F -Risc integritat.xls)

Fruit d'aquest anàlisis adjuntarem en el present document els Resultats finals del Risc en les diferents dimensions. Ho mostrarem en el següent apartat.

10.3. RESULTATS FINALS DEL RISC

Així doncs podrem obtenir la següent taula de Resultats Finals de l'anàlisi de RISC, comentem a continuació per la Dimensió de Confidencialitat, Càlcul Risc Confidencialitat. adjuntarem a continuació el resum també de les altres dimensions. Els càlculs del Risc en tots els casos es als annexos D,E,F, en la carpeta adjunta, al present document.

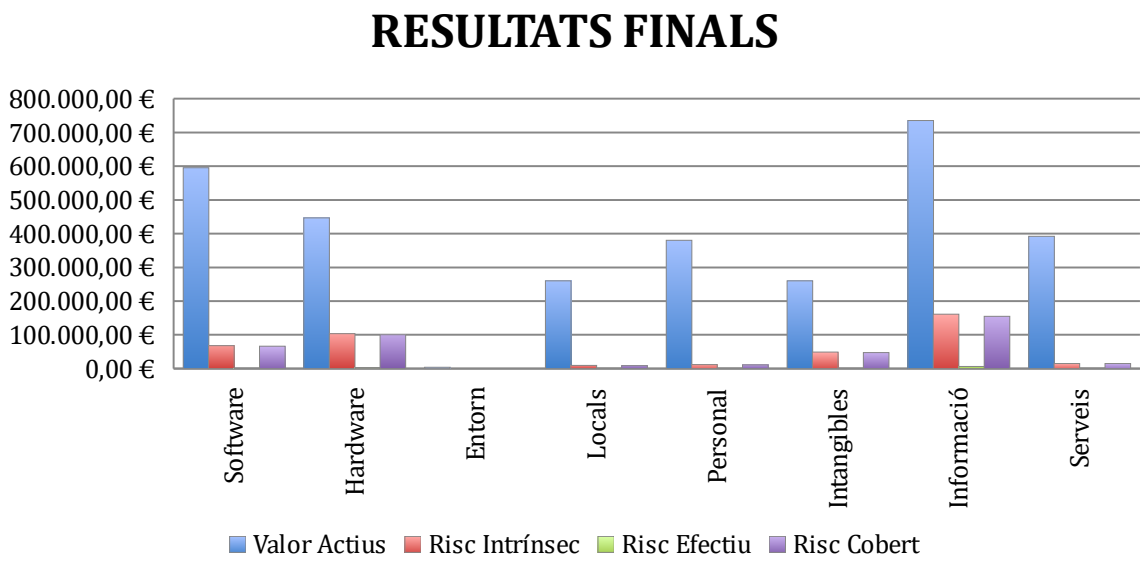
TAULA D'ANALISI DE RISC PER LA DIMENSIÓ DE CONFIDENCIALITAT.

En aquesta taula classifiquem els Actius per Tipus. I Calculem el Valor total dels mateixos per Tipus. Mostrarem

- El risc Intrínsec de cadascun dels Actius per Tipus.
- El Risc Efectiu un cop aplicades les Salvaguardes sobre les Amenaces
- I El risc cobert que serà el que s'ha aconseguit protegir, per tant la resta d'ambdós.

TIPUS	VALOR DELS ACTIUS	RISC INTRÍNSEC	RISC EFECTIU	RISC COBERT
Software	595.000,00 €	67.141,60 €	1.238,85 €	65.902,75 €
Hardware	446.000,00 €	102.957,00 €	2.757,20 €	100.199,80 €
Entorn	3.000,00 €	0,00 €	0,00 €	0,00 €
Locals	260.000,00 €	8.525,40 €	637,97 €	7.887,43 €
Personal	380.000,00 €	11.354,40 €	825,77 €	10.528,63 €
Intangibles	260.000,00 €	48.054,80 €	1.112,18 €	46.942,62 €
Informació	735.000,00 €	160.352,94 €	5.765,42 €	154.587,52 €
Serveis	392.000,00 €	14.667,48 €	738,15 €	13.929,33 €

MOSTRAREM UN GRÀFIC DELS RESULTATS.

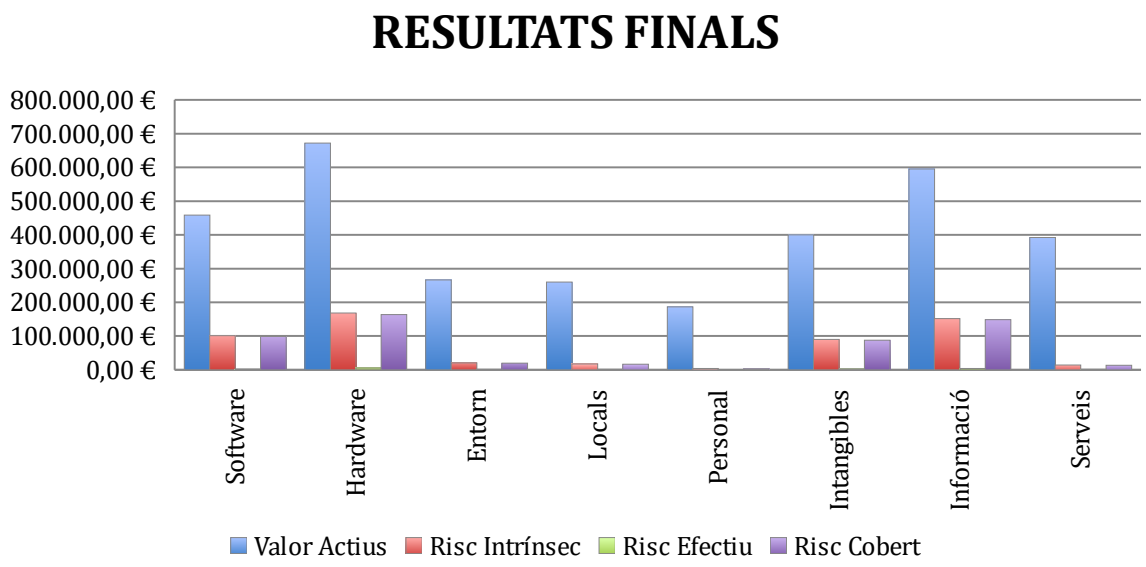


TAULA D'ANALISI DE RISC PER LA DIMENSIÓ DE DISPONIBILITAT.

Mostrarem els resultat del Anàlisis de Risc per la Dimensió de Disponibilitat, la fulla de càlcul amb l'avaluació dels diferents valors la podem trobar a la carpeta Annexos adjunta el present document. O al Següent Link. Annex E Risc Disponibilitat.

TIPUS	VALOR DELS ACTIUS	RISC INTRÍNSEC	RISC EFECTIU	RISC COBERT
Software	458.000,00 €	100.338,36 €	1.852,63 €	98.485,73 €
Hardware	672.000,00 €	167.907,48 €	4.683,68 €	163.223,80 €
Entorn	266.000,00 €	19.791,18 €	632,53 €	19.158,65 €
Locals	260.000,00 €	16.569,00 €	1.035,74 €	15.533,26 €
Personal	186.000,00 €	2.943,96 €	255,57 €	2.688,39 €
Intangibles	400.000,00 €	89.532,00 €	2.313,00 €	87.219,00 €
Informació	595.000,00 €	151.237,44 €	3.374,86 €	147.862,58 €
Serveis	392.000,00 €	13.756,56 €	768,67 €	12.987,89 €

MOSTRAREM UN GRÀFIC DELS RESULTATS.

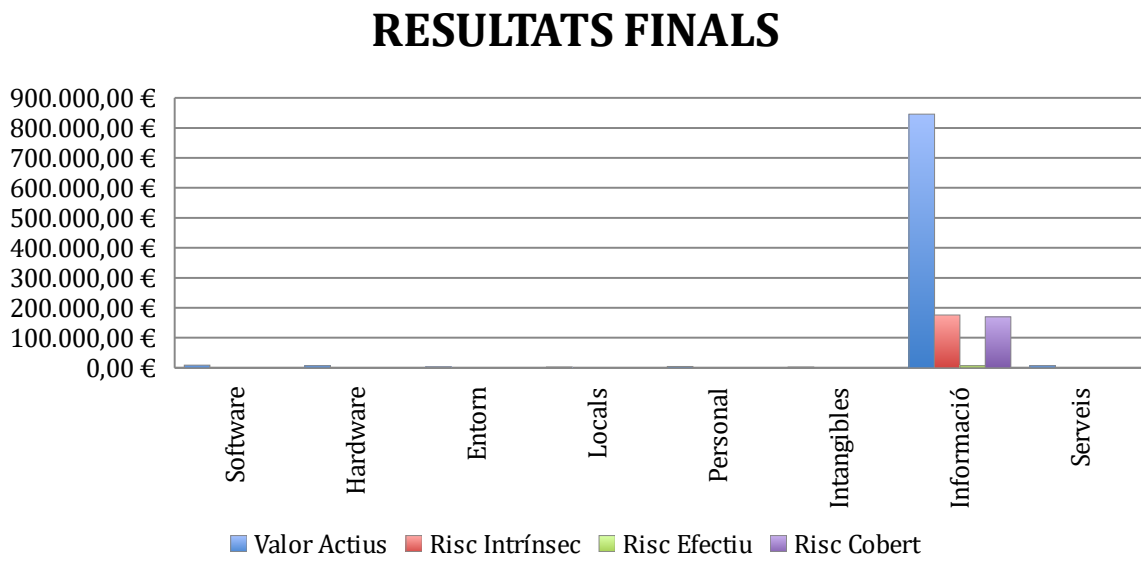


TAULA D'ANALISI DE RISC PER LA DIMENSIÓ D'INTEGRITAT

Mostrarem els resultat del Anàlisis de Risc per la Dimensió d'Integritat, la fulla de càlcul amb l'avaluació dels diferents valors la podem trobar a la carpeta Annexos adjunta el present document. O al Següent Link. Annex F. Risc Integritat.

TIPUS	VALOR DELS ACTIUS	RISC INTRÍNSEC	RISC EFECTIU	RISC COBERT
Software	8.000,00 €	0,00 €	0,00 €	0,00 €
Hardware	6.000,00 €	0,00 €	0,00 €	0,00 €
Entorn	3.000,00 €	0,00 €	0,00 €	0,00 €
Locals	2.000,00 €	0,00 €	0,00 €	0,00 €
Personal	4.000,00 €	0,00 €	0,00 €	0,00 €
Intangibles	2.000,00 €	0,00 €	0,00 €	0,00 €
Informació	846.000,00 €	175.335,66 €	6.320,87 €	169.014,79 €
Serveis	6.000,00 €	0,00 €	0,00 €	0,00 €

MOSTRAREM UN GRÀFIC DELS RESULTATS.



Cal destacar que en la dimensió d'integritat entenem aquesta cop la integritat de les **dades**. Així doncs tot l'anàlisi l'hem enfocat a la Informació.

En els tres casos seria la direcció la que haurà de revisar el Sistema i acceptar el Risc Efectius, ser conscient de l'aplicació de les Salvaguardes oportunes i en tot cas decidir si acceptar el Risc o tractar-lo, assignant recursos per tal tasca. Aquest procés el realitzarem posteriorment, en la fase de revisió per la direcció FASE 6 del present document.

11. FASE 4. PROJECTES D'ALINEACIÓ AMB ELS OBJECTIUS DEL PLA DIRECTOR

Per tal de reduir el nivell de risc i alinear-nos amb els objectius del Pla director de la Organització, definirem una sèrie de Projectes de Seguretat de la Informació que ens permetran alinear-nos també amb els objectius del negoci i les polítiques de la direcció i que estan previstos dur a terme en el cicle 2017-2018. Seguint amb el pla de Millora continua proposat per la Mutua interuniversitària.

Cal destacar abans de la posta en marxa dels diferents projectes plantejats, en primer lloc es portarà a terme una Reunió Ordinària del Comitè de seguretat amb la junta directiva on s'exposaran degudament els diferents projectes sorgits fruits de les necessitats de millora del Sistema.

Els Assistents a la reunió seran: Director General, Director de Tics, Director de Qualitat i Medi ambient, Responsable de Seguretat, Director financer i Director D'organització.

A continuació mostrarem els diferents projectes proposats, definits per les diferents fases, mostrarem també una quantificació econòmica, basant-nos en el prerequisit de la direcció on se'ns ha especificat clarament que en la mesura del possible no havien de suposar un esforç econòmic addicional als recursos salarials de la pròpia organització.

Posteriorment mostrarem un organigrama de planificació dels diferents projectes definint una estimació de les seves línies de temps durant el període definit. Cal destacar que tot i que els projectes estiguin definits per el cicle 2017-2018, hi ha projectes que degut a la seva natura es perllongaran en el temps per la qual convindrà gestionar una ampliació de projecte per a propers cicles. Tenint en compte aquesta natura podem classificar els projectes a curt-mig termini o a llarg termini.

Per tal de mitigar els nivells de risc i limitacions associades a les circumstàncies actuals de la organització i enfortir les salvaguardes relacionades exposarem doncs els següents projectes.

- PROJECTES A MIG-CURT TERMINI:
  - PROJECTE D'ENCRIPTACIÓ DE PORTATILS.
  - PROJECTE DE CONTROL DE SEGURETAT FÍSICA A NIVELLS DE PORT DELS SWITCHOS.
  - PROJECTE D'IMPLANTACIO´ D'UN SISTEMA INTEGRAT D'INVENTARI D'EQUIPS.
  - PROJECTE D'ORGANITZACIÓ DE LA INFORMACIÓ SENSIBLE ALS SERVIDORS
  - PROJECTE DE CLASSIFICACIÓ DEL CICLE DE VIDA DE LA INFORMACIÓ.

- PROJECTES A LLARG TERMINI
  - PROJECTE DE FORMACIÓ D'USUARIS.
  - PROJECTE DE PROPOSTA D'AMPLIACIÓ, E INTEGRACIÓ DELS SISTEMES DE GESTIÓ DE LA ORGANITZACIÓ.

El desenvolupament complert de tots els projectes D'alineació amb ells Objectius del pla director els podem trobar a l'Annex I. (Annex I. Projectes d'Alineació amb els Objectius del Pla Director).

Mostrarem en la següent taula com pretenem que millorin les competències en els riscos relacionat amb cadascun dels projectes, en primer lloc definint quines son les salvaguardes que reforcen, quines son les amenaces relacionades i en quina dimensió, un cop implementat el projecte avaluarem el risc i posteriorment a la revisió del sistema per la direcció justificarem com han variat els riscos aplicant els projectes relacionats.

PROJECTE	SALVAGUARDES QUE REFORÇAREM	AMENACES RELACIONADES	DIMENSIÓ
PROJECTE D'ENCRIPTACIÓ DE PORTATILS.	• Seguretat dels equips • Informàtica mòbil i teletreball • Controls criptogràfics	Fuita d'informació	Confidencialitat
		Accés no autoritzat	Confidencialitat
		Divulgació de la informació	Confidencialitat
		Manipulació de la informació	Integritat
PROJECTE DE CONTROL DE SEGURETAT FÍSICA A NIVELLS DE PORT DELS SWITCHOS.	• Controls d'accés a xarxa • Gestió de les xarxes • Control d'accés a Xarxa	Fuites d'informació	Confidencialitat
		Manipulació de la configuració	Integritat
		Accés no autoritzat	Confidencialitat
PROJECTE D'IMPLANTACIÓ D'UN SISTEMA INTEGRAT D'INVENTARI D'EQUIPS.	• Seguretat dels equips • Controls generals • Gestió de xarxes	Errors del Administrador	Integritat
		Errors d'actualització de hardware	Disponibilitat
PROJECTE D'ORGANITZACIÓ DE LA INFORMACIÓ SENSIBLE ALS SERVIDORS	• Controls generals • Gestió interna de suports i recuperació. • Gestió d'accés dels usuaris • Seguiment d'accessos i usos	Degradació dels suports d'emmagatzemament	Integritat Disponibilitat

	del sistema • Seguretat dels fitxers del sistema		
		Errors de configuració o de disseny	Disponibilitat Confidencialitat
PROJECTE DE CLASSIFICACIÓ DEL CICLE DE VIDA DE LA INFORMACIÓ.	• Utilització i seguretat dels suports d'informació • Classificació de la informació	Erros de configuració o de disseny	Disponibilitat
PROJECTE DE FORMACIÓ D'USUARIS.	Formació d'usuaris	Errors dels usuaris	Disponibilitat Integritat Disponibilitat
		Difusió de software malintencionat o virus	Integritat
		Fuites d'informació	Confidencialitat
		Destrucció de la informació	Integritat
		Divulgació de la informació.	Confidencialitat
		Manipulació de la configuració	Integritat
		Suplantació d'identitat	Confidencialitat
		Accés no autoritzat	Confidencialitat

		Robatoris d'equips	Disponibilitat
		Enginyeria Social	Confidencialitat
PROJECTE DE PROPOSTA D'AMPLIACIÓ, E INTEGRACIÓ DELS SISTEMES DE GESTIÓ DE LA ORGANITZACIÓ.	• Estructura per la seguretat de la informació • Procediments i responsabilitats d'operació • Consideracions sobre l'auditoria de sistemes	Es tractara ` de millores mes enllà del àmbit de les amenaces definides en el SGSI • Cicle de Millora continua. • No es duplicaran esforços • Mateixa importància • Comunicació i Sinergies • Estalvi en temps i costos d'auditoria	En totes les dimensions de la organització.

11.1. DIAGRAMA DE GANTT PROJECTES

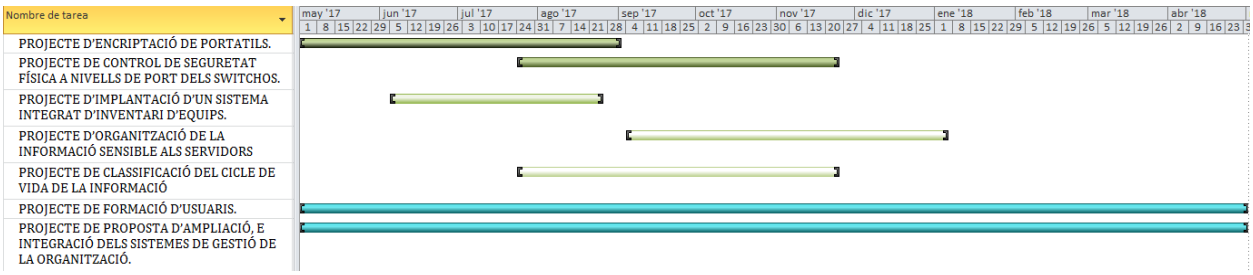
Mostrarem a continuació un diagrama de Gantt dels diferents projectes plantejats per cicle en curs del SGSI.

En primer lloc definirem les tasques i les duracions estimades totals dels projectes. Com hem comentat en línia amb l'SGSI existeixen projectes continus en el temps, en quant a PDCA, no obstant definim una data final de la Implantació del mateix.

NOM DE LA TASCA	DURACIÓ	COMENÇAMENT	FÍ
PROJECTE D'ENCRIPTACIÓ DE PORTATILS.	90 dies	lun 1/5/17	vie 1/9/17
PROJECTE DE CONTROL DE SEGURETAT FÍSICA A NIVELLS DE PORT DELS SWITCHOS.	90 dies	lun 24/7/17	vie 24/11/17
PROJECTE D'IMPLANTACIÓ D'UN SISTEMA INTEGRAT D'INVENTARI D'EQUIPS.	60 dies	lun 5/6/17	vie 25/8/17
PROJECTE D'ORGANITZACIÓ DE LA INFORMACIÓ SENSIBLE ALS SERVIDORS	90 dies	lun 4/9/17	vie 5/1/18
PROJECTE DE CLASSIFICACIÓ DEL CICLE DE VIDA DE LA INFORMACIÓ	90 dies	lun 24/7/17	vie 24/11/17
PROJECTE DE FORMACIÓ D'USUARIS.	262 dies	lun 1/5/17	mar 1/5/18
PROJECTE DE PROPOSTA D'AMPLIACIÓ, E INTEGRACIÓ DELS SISTEMES DE GESTIÓ DE LA ORGANITZACIÓ.	262 dies	lun 1/5/17	mar 1/5/18

Alguns dels projectes definits requereixen d'un projecte associat per portar-se a terme, com per exemple el projecte d'implementació d'un sistema d'inventari d'equips s'ha de desenvolupar en paral·lel amb el projecte de Control de seguretat física a nivell de ports dels Switchos.

A continuació mostrarem Gràficament amb el diagrama de Gantt aquestes, fluxos.



12. FASE5. AUDITORIA DE COMPLIMENT DE LA ISO/IEC 27001:2013

Durant la realització d'aquesta fase del TFM, haureu de realitzar un anàlisis de compliment de l'organització davant la ISO: IEC 27001:2013, analitzant el control, maduresa i nivell de compliment.

OBJECTIU
L'objectiu del procediment d'auditoria es establir i descriure com es porten a terme les auditories internes del sistema de gestió de la seguretat de la Informació, com es registren les desviacions i com son acordades, complimentades i verificades les respectives accions correctives i preventives.

El resultat de l'auditoria ha de permetre

a) Avaluar el nivell de compliment del Sistema de Gestió de Seguretat de la informació de Mutua Interuniversitària, segons la Norma 27001:2013 i els criteris d'auditoria.
b) Avaluar també la conformitat de la política de seguretat, amb les especificacions de la norma Internacional ISOIEC 27002:2013 que agrupa 14 dominis, 35 Objectius de Control i 114 Controls, i amb els requisits del SGSI establerts per la direcció.
c) Avaluar el nivell de Maduresa dels controls, un cop implementats els projectes d'alineació amb els objectius del pla director.
d) Verificar que la SGSI S'ha implementat, es manté i s'executa de forma eficaç
e) Verificar que el Procés d'auditoria es adequat pels actius i el seu valor, així com les amenaces i els riscos de la Organització
f) Verificar també els registres de revisió del anàlisis de Riscos.
g) Extreure coneixement de la pròpia organització i opcions per la millora continua del SGSI.

ABAST
L'abast de l'auditoria Interna son els Sistemes d'informació que suporten tots els processos de negoci:

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

I que es presten des de Seu Corporativa d'acord amb el document d'aplicabilitat vigent així com el centre de contingència de Manresa

PERFILS AFECTATS
Els perfils involucrats en el procés d'auditoria de compliment son:

- Direcció
- Responsable de Sistemes i Seguretat
- Responsable d'Organització
- Responsable Financer
- Responsable d'Enginyeria
- Responsable d'Infraestructures.
- Responsable d'LOPD
- Auditor Interns

RESPONSABILITAT

Les auditories internes del SGSI son responsabilitat del Responsable de Seguretat o per qualsevol altre membre del equip d'auditors qualificats que hagi estat designat per ell. L'auditor designat ho serà amb la condició de que no tingui responsabilitat directes en el àrea de treball o departament que serà auditat. L'auditor intern haurà de tenir un curs d'auditor Intern, preferiblement CISA.

PERIODICITAT

Cada any es realitzara` una auditoria integra de compliment amb la norma ISO/UNE 27001:2013. Per altre banda, les auditories internes del SGSI es realitzaran mitjançant mostrejos dels diferents controls de la ISO/UNE 27002:2013, periòdicament, implementant cada any una revisió de tots els objectius de control i com a mínim cada dos anys de tots els 114 controls.

12.1. PLA D'AUDITORIA

Els plans d'auditoria realitzats s'arxivaran a la BBDD del SGSI, al apartat de documents.
Aquest es establert pel Responsable de Seguretat, o per qui ell designi, notificant amb un temps prudencial d'antelació a la primera auditoria programada.

Quan es defineixi el calendari d'auditories o modificacions sobre el mateix, el responsable de seguretat enviarà un marcador al equip d'auditors i als responsables dels departaments implicats pel seu coneixement.

S'establirà l'abast de l'auditoria definint els processos que s'auditaran. Els criteris de cada auditoria els recollirà el cap d'auditors en funció del seu coneixement del SGSI.

A mes de les auditories programades, es podran concertar auditories ocasionals sota la supervisio´ del Responsable de Seguretat, en resposta a una situacio´ insatisfactòria o increment considerable de incidències de seguretat.

La Direccio´ podra` definir auditories no programades en aquells casos que consideri necessari, prèvia notificació per escrit via Mail.

Per realitzar les auditories internes es mantindrà format a un equip d'auditors. La formació serà oferida pel Responsable de Seguretat o la persona que aquest designi a tals efectes.
La capacitat del formador d'auditors estarà avalada pel Responsable de Seguretat i/o pels cursos que a tals efectes hagi realitzat el formador.

Podem trobar el pla d'auditoria adjunt al present document a "l'Annex K. Pla d'auditoria Interna"

12.2. FASES I EXECUCIÓ DE L'AUDITORIA

Les auditories internes del SGSI es realitzaran seguint les següents fases:

PREPARACIÓ DE L'AUDITORIA
L'auditor prepararà una taula amb els punts a auditar, segons el format de la Norma, per a ser emprada a l'auditoria a la que es tingui en compte el SOA i la Anàlisis diferencial o de maduresa dels diferents controls, procediments, objectius i altre documentació rellevant del departament, així com desviacions pendents d'auditories anteriors. En aquest cas al tractar-se de la primera auditoria de Mutua Interuniversitària, no es tindran en compte aquests últims.

Podem trobar la selecció de Controls d'Auditoria de la norma ISO/IEC 27002:2013 al document "Annex L. Selecció de Controls d'auditoria"

L'auditoria de cada activitat o departament la realitzarà un auditor aliè a la mateixa.
Igualment podrà emprar les notes d'auditoria per anotar les desviacions, punts de millora i punts forts.

NOTIFICACIÓ DE L'AUDITORIA
L'auditor haura` de notificar qualsevol auditoria que hagi de realitzar als caps de departament responsables de les àrees a auditar, amb un temps prudencial d'antelació, per tal de poder concertar un termini i horari adequat per a la seva realització.

REUNIÓ PRELIMINAR
L'auditor i els caps de departament tindran una reunió preliminar on es confirmarà l'àmbit de l'auditoria, el programa i tot el referent a desviacions i accions correctores.

EL PROCÉS D'AUDITORIA
Durant l'auditoria, l'auditor haurà d'estar acompanyat, preferiblement, d'un representant del àrea que està sent auditada. Quan l'auditor detecti una deficiència la comentarà amb el responsable del àrea en qüestió, arribant a un acord sobre l'evidència dels fets observats, s'hauran d'anotar les evidències o exemples que demostrin la desviació. Així mateix, es comentaran i s'anotaran les possibles millores detectades.
Durant el procés d'auditoria es verificaran els controls, el grau d'implantació i la seva eficàcia. A mesura que es vagin auditant els punts de la norma es registraran aquests.

L'INFORMÉ D'AUDITORIA
Un cop finalitzada l'auditoria, l'auditor cap recollirà les taules de punts auditats amb les possibles notes de desviació i realitzara` un informe resumint-les totes, identificant clarament el departament auditat, la data d'auditoria i es detallaran els següents punts:

- Detalls de les desviacions, millores, indicant títol, numero i documents als que es refereix.
- Lloc on s'han detectat les desviacions o millores o punts forts.
- Detalls de les accions correctores/preventives acordades i data a la que hauran de ser corregides. Aquestes derivades de l'auditoria seran tramitades tal i com s'especifica el procediment d'accions correctives i preventives.

- L'informe d'auditoria serà editat en el sistema documental del SGSI, i arxivat a l'apartat de documents.
- També es disposarà d'un arxiu digitalitzat, fruit de les notes de desviació pertanyents a les auditories i les taules de punts auditats. Aquest arxiu estarà sota la responsabilitat del Responsable de Seguretat.

SEGUIMENT I TANCAMENT DE L'AUDITORIA INTERNA.
De totes les possibles accions correctives i/o preventives derivades de l'auditoria interna, es desenvoluparà un PAC, Pla d'Accions Correctives i hauran de ser seguides pel cap d'auditoria, no considerant-se l'auditoria interna tancada fins que totes elles estiguin tancades.

Tant el desenvolupament de l'auditoria com l'informe final de la mateixa el podem trobar a l'annex "Annex J Auditoria de Compliment de la ISO" adjunt al present document.

12.3. RESUM DELS RESULTATS DE L'AUDITORIA

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.

Caldrà implementar doncs un PAC, Pla d'accions Correctives per tal de portar a terme les accions adequades per gestionar aquestes desviacions.

Aquest escenari ens porta a resumir que el Sistema de Gestió reflecteix un escàs nombre d'incidències rellevants, tenint en compte el grau de madures del propi Sistema de Gestió, donat el punt en el que aquest es troba , els nivells de disponibilitat del sistema i el bon resultat de les mesures dels indicadors, així com la consecució dels objectius fixats per la Organització. Sent aquells objectius on no existeix una partida econòmica associada els aspectes més rellevants d'aquesta auditoria,

Degut a la natura particular de la Organització. , en quant a polítiques organitzacionals i restriccions pressupostaries, exposades per la direcció de la mateixa s'observa un fre important en aquells aspectes de millora que poden requerir una inversió econòmica associada. Tot i així s'ha destinat una important part dels recursos de personal, a la posta en marxa de nous objectius i projectes que complementen les millores de seguretat cap a una convergència amb els objectius estratègics de la Organització.

En general es pot apreciar una preocupació de la Organització per mantenir el sistema com una eina efectiva, alineada amb els objectius estratègics i que assegura garantir la seguretat de la Organització.

13. FASE6. PRESENTACIÓ DE RESULTATS I ENTREGA DELS INFORMES.

En Aquesta Sisena fase del projecte portarem a terme els següents punts.

- Consolidació dels resultats obtinguts durant el procés d'anàlisis.
- Realització dels informes
- Presentació executiva a la Direcció
- Entrega del projecte final.

Per realitzar aquestes tasques desenvoluparem en primer terme el document de Revisió del Sistema per la Direcció. En aquest document presentarem formalitzat emprant el format de la Fase2 el Resum de tot el projecte per una fictícia Direcció, que ha d'esser la que ha d'aprovar el sistema i proporcionar els recursos necessaris per atorgar-li recolzament i continuïtat a la SGSI.

En segon terme prepararem una presentació pel projecte en format PowerPoint amb la qual realitzarem un vídeo de presentació del Projecte Final de Màster. L'adjuntarem també al directori dels Annexos amb el títol. Presentació TFM.

Aquesta Presentació pretén per un costat ser una síntesi, del treball realitzat durant tot aquest període, entenent l'enfoc del resultat cap a una avaluació de les fases implementades que seran resumides en la presentació.

Per altre costat també pretén recollir la presentació dels resultats del projecte, entenent l'enfoc del resultat amb una orientació cap a la direcció de la Mutua Interuniversitària, sobre la que s'ha implantat l'SGSI.

CONCLUSIONS

Com a conclusions del present treball i del procés d'implantació del SGSI en la empresa Mutua Interuniversitària, podem concloure que s'ha posat en marxa el cicle de millora continua, PDCA, de la SGSI, complint les expectatives de la direcció i alineant el pla director del mateix amb els objectius i la política de la direcció de la Organització.

S'han portat a terme els objectius definits mitjançant els projectes implantats en la Organització tant a curt-mig termini com projectes continus a llarg termini, que engloben mes d'un cicle del sistema de gestió.

Un gran nombre de controls ja es troben implantats i contenen un indicador per realitzar la avaluació del mateix. Hem aconseguit millorar l'estat de maduresa dels mateixos passant en una escala del Model de "Capacitat i Maduresa" CMM, d'un estat inicial a un estat Definit.

S'ha involucrat i format al personal que forma part implicada directament en el Sistema de Gestió i al personal en general de tota la Organització.

Podem discernir que la Organització ha entès el SGSI i que existeix un recolzament i un gran interès per part de la Direcció tant de cultura com de recursos per permetre la continuïtat del Sistema, assegurant la facilitat i vies de comunicació amb el Comitè de Seguretat.

El sistema ha demostrat la seva eficàcia i complir amb els requisits establerts per les normes de referencia aplicades i normatives legals.

A NIVELL LECTIU.

Hem reforçat els coneixements sobre tots els cicles de Implantació, manteniment i gestió del Sistema de Gestió de Seguretat de la Informació.

He pogut millorar les capacitats i aplicar els coneixements obtinguts cap al meu àmbit laboral, essent aquest projecte un enfortiment de les bases necessàries per portar a terme el projecte d'integració dels diferents sistemes de Gestió de la seguretat en la meva organització, que adjuntem en aquest document a partir del punt 14 i que pretén ser l'inici d'una continuïtat del mateix.

A NIVELL PERSONAL

Per altre banda sense ser menys important, ha estat un autèntic plaer el poder comptar amb el recolzament i coneixements, del tutor del projecte Arsenio Tortajada Gallego que ha col·laborat amb la realització del mateix i m'ha aportat sempre una visió interessant.

Concloc, que ha estat una gran experiència de vida el realitzar un màster com el MISTIC amb els grans professionals que han demostrat ser durant tot aquest temps, els tutors de les diferents assignatures de la UOC.

Gràcies a tots, m'enduc un tros de cadascú de vosaltres en aquest viatge del coneixement.

14. DOCUMENT DE PROPOSTA D'AMPLIACIÓ DEL PROJECTE. INTEGRACIÓ DELS SISTEMES DE GESTIÓ D'UNA ORGANITZACIÓ.

MOTIVACIÓ DE LA PROPOSTA

Aquesta idea prové de la problemàtica que trobem a la nostra organització, on tenim per un costat el Sistema integrat de gestió que agrupa la ISO 9001 i la ISO 14001, Qualitat i Medi ambient.

La idea inicial seria incloure en el Sistema Integral de Gestió també l'auditoria de Seguretat, el Esquema Nacional de Seguretat (ENS), i Oshas (18001), La Norma de Prevenció.

El procés d'unificació pretendria portar a terme l'assegurament dels processos de la organització en aquestes dimensions, que tanmateix serien perpendiculars als processos de la mateixa.

Els punts que tindríem en compte en aquesta ampliació serien.

- Estudi dels Beneficis de la unificació dels Sistemes de Gestió.
- Estudi dels aspectes comuns entre les auditories.
- Capacitació per portar a terme la Integració
- Planificació de les fases i estratègia d'integració
    - Anàlisis dels Processos de Negoci
    - Anàlisi d'Integració del SGSI
    - Estudi de Creació de nous Rols
    - Anàlisi dels Estats de Maduresa dels diferents sistemes.
- Planificació dels Recursos
- Procés d'unificació del SGSI
    - Estudi d'unificació de les normes.
- Estudi d'unificació dels sistemes documentals
    - LA Anàlisis de Riscos Conjunt.
    - La gestió de les no conformitats
- Un sol procés d'auditoria conjunta.
- El PDCA d'un SGSI.
    - Mesura de la maduresa en paral·lel, de les diferents normatives.
- L'aplicabilitat de les normatives als processos de negoci.
- Desenvolupament d'una plataforma del Sistema de Gestió i Documental.
- Conclusions.

15. ESTUDI DELS BENEFICIS D'INTEGRACIÓ DELS SISTEMES DE GESTIÓ.

Que ens aporta la integració dels sistemes de Gestió? Aquesta integració ens aporta els següents avantatges.

- **Cicle de Millora continua.** Es el nexe d'unió mes fort entre els estàndards.
  - La millora es pot plantejar des de una visió conjunta, i durant el seguiment dels plans d'acció i dels indicadors.
  - També S'evitaran danys colaterals en la gestió de les incidències que pot provocar una auditoria sobre una altre. (la solució d'un problema relatiu a una auditoria a expenses de disminuir la seguretat en aspectes d'una altre).

- **No es duplicaran esforços.** Existeixen molts punts comuns entre les normatives i per tant es poden planificar junts, tals com:
  - Les auditories internes
  - La gestió de la documentació
  - La revisió per part de la direcció.
  - Tot es pot unificar en un sol informe.
  - Tractament de la millora continua o PDCA.
  - Tractament de les no conformitats.

- **Mateixa importància.** Al integrar els sistemes anteriors podem donar la mateixa importància a totes les normatives i certificacions, tant qualitat com gestió mediambiental com a la seguretat, aquesta acostuma a ser una bona visió organitzativa.

- **Comunicació i Sinergies.** La integració millora la comunicació i les sinergies en les diferents àrees de treball.

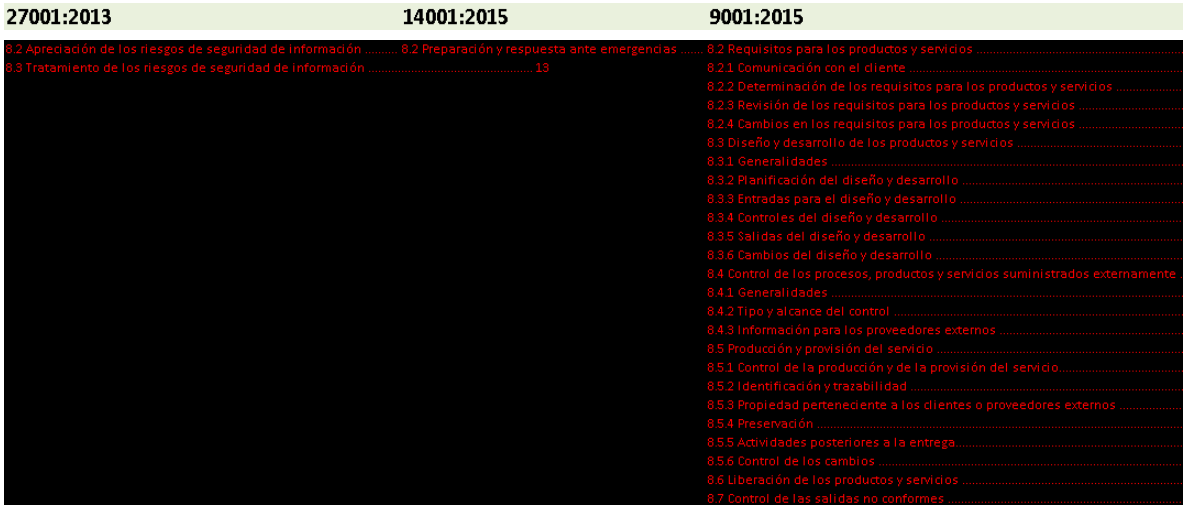
- **Estalvi en temps i costos d'auditoria.** Si la mateixa entitat consent realitzar auditories de forma conjunta, es redueix la inversió en temps i diners requerits, Si l'auditor d'ISO 9001, comprova que el pla de formació es correcte i coherent, no es necessari que l'auditor de ISO 27001 torni a revisar aquest document.

16. ANÀLISI I GRAFICACIÓ, D'ASPECTES COMUNS, DIRECTES I COLATERALS DE LES DIFERENTS NORMES.

Per tal de fer un anàlisi dels aspectes comuns entre les diferents normatives per una posterior unificació dels Sistemes de Gestió desenvoluparem un Excel que adjuntarem a l'Annex B del present document.

En aquesta fulla de càlcul analitzarem els elements comuns a totes les auditories i els elements que anomenarem col·laterals que son aquells que tot i compartir la natura hauríem de concretar per cadascuna d'aquestes.

Fruit del present anàlisis determinem. La part no comuna esdevindria del punt 8 de les normes endavant.



Resulta important destacar que la màxima eficàcia del anàlisis del context s'aconsegueix quan es s'aconsegueix involucrar a totes les parts interessades, com per exemple, els representants de la direcció dels sistemes de gestió a Integrar, les funcions implicades en el sistema que es considerin necessàries i la alta direcció.

Actualment podem graficar una integració dels sistemes de Gestió, qualitat i medi ambient.

17. CAPACITACIONS NECESSARIES PER PODER PORTAR A TERME LA INTEGRACIÓ DELS SISTEMES DE GESTIÓ.

Entenem que la integració dels diferents sistemes de Gestió no es pot portar a terme nomes per una persona sino´ que ha de formar-se un grup de treball capacitat i amb un coneixement de gestió global de la Organització.

Es per tant que a priori documentarem una sèrie de capacitació mínima que exigirem per tal d'assegurar.

- Titulació independent en Auditories de Seguretat. (MISTIC, AENOR, CISA)
- Capacitació en Auditories de Medi Ambient
- Capacitació en Auditories de Qualitat
- Capacitació en Auditories de Prevenció o Tècnic de Prevenció
- Formació en Gestió de Riscos Empresarials.
- Capacitat de obtenir una visió global de la organització i de gestió de Processos.

18. PLANIFICACIÓ DE LES FASES I ESTRATÈGIA D'INTEGRACIÓ.

18.1. ANÀLISI DE LA ESTRATÈGIA D'INTEGRACIÓ.

Entenem que la clau per una bona integració es sobretot una bona planificació. El Projecte no ha de basar-se únicament en l'estat actual de la organització, o en termes de compliment dels requisits de les normes. Sinó que ha de ser capaç de detectar accessos directes i madurs, dèficits dels sistemes, estats de maduresa, necessitats d'inclusió d'indicadors, millores en els controls, i possibles col·lisions entre les aplicacions del les normes que s'han de mesurar per poder-les gestionar.

Per altre banda la clau per l'estalvi per accelerar la integració es l'aplicació dels requisits comuns de les normes. Recursos humans, control de documents, objectius i planificacions o accions correctives. Així doncs podrem destacar:

- **Context de la Organització**. Identificació dels problemes interns i externs a la empresa. Però des de diferents perspectives. Per exemple, la ISO 9001, es centra en la qualitat i la ISO 27001 en la Seguretat de la Informació.
- **Parts Interessades i requisits.** La organització haurà de determinar les parts interessades i els requisits relacionats amb totes les normes. Una idea inicial vindria determinada per identificar en un llistat el que determinen els diferents sistemes actuals i parts interessades.
- **Responsabilitat i autoritat per ser identificats.** Els rols i les responsabilitats dins del Sistema de Gestió Integrat son diferents, però i han de ser definits de nou.
- **Competència, sensibilització, comunicació, control del sistema documental i registres.** Tots aquests requisits son comuns entre totes les normes per tant poden abordar-se de la mateixa manera i al mateix temps.
- **Auditoria interna i revisió de la direcció**. Tot i que els requisits per ser auditats son diferents la forma en la que es porta el procés es la mateixa. Depenent de la mida de l'empresa i dels seus processos, l'auditoria interna o revisió de la direcció es poden fer al mateix temps.
- **Totes les normes requereixen sistemes per accions correctives i de no conformitat.** Així doncs el procés de tractament de les no conformitats i accions correctives poden ser el mateix per tots els estàndards, no hi ha cap raó aparent per separar-los.

Em de tenir present que per tal d'integrar les normes en un sol Sistema de Gestió Integrat (SGI), s'ha de satisfer el mes exigent de tots ells.

L'ANNEX SL i L'ESTRUCTURA BÀSICA D'INTEGRACIÓ

Tot i que totes les normes ISO fins al moment tenien aspectes comuns i adoptaven el cicle PDCA, moltes aplicaven requisits similars de mètodes diferents. L'Annex SL va ser desenvolupat per tal de posar fi a aquest problemes d'aplicació, mitjançant una

estructuració d'alt nivell idèntic per totes les normes, garantint una base que facilita la integració, lectura e interpretació i posterior integració en les Organitzacions.

L'Annex SL descriu el context per un sistema de gestió genèric deixant de banda la addició dels requisits específics de les àrees per a transformar-se en una norma de sistema de gestió de qualitat, o de Seguretat Però quins elements composen l'Annex SL?
Aquest està composat de varies parts. Analitzarem l'apèndix 2. Aquest es dividirà en 3 sectors.

- Estructura d'alt Nivell
- Text base idèntic
- Termes i definicions comuns

La estructura d'alt nivell ha distribuït les clàusules en 10 seccions, conforme l'enfoc del PDCA de mode que resultin en una seqüencia lògica respecte els requisits dels sistemes de gestió, tals com la informació documentada, les accions correctives, les auditories internes o la revisió per part de la direcció entre altres.
L'estructura tindrà la següent forma:

- AMBIT
- REFERÈNCIES NORMATIVES
- TERMES I DEFINICIONS
- CONTEXT DE LA ORGANITZACIÓ
  - Parts interessades, marc normatiu..
- DIRECCIÓ
  - Compromís amb la direcció, política, funcions, responsabilitats i autoritat
- PLANIFICACIÓ
  - Gestió de riscos i oportunitats, objectius i planificació → P (del PDCA)
- SUPORT
  - Recursos, formació, presa de consciencia, comunicació, i tot el relacionat amb la gestió de la documentació del SG)
- OPERACIONS
  - Apartat amb tots els requisits específics de cada norma → D (del PDCA)
- EVALUACIÓ DEL ACOMPLIMENT
  - Seguiment i mesura, anàlisis de dades, auditoria Interna i revisió per la direcció → C (del PDCA)
- MILLORES
  - Inclou no conformitats i accions correctives i millora continua → A (del PDCA)

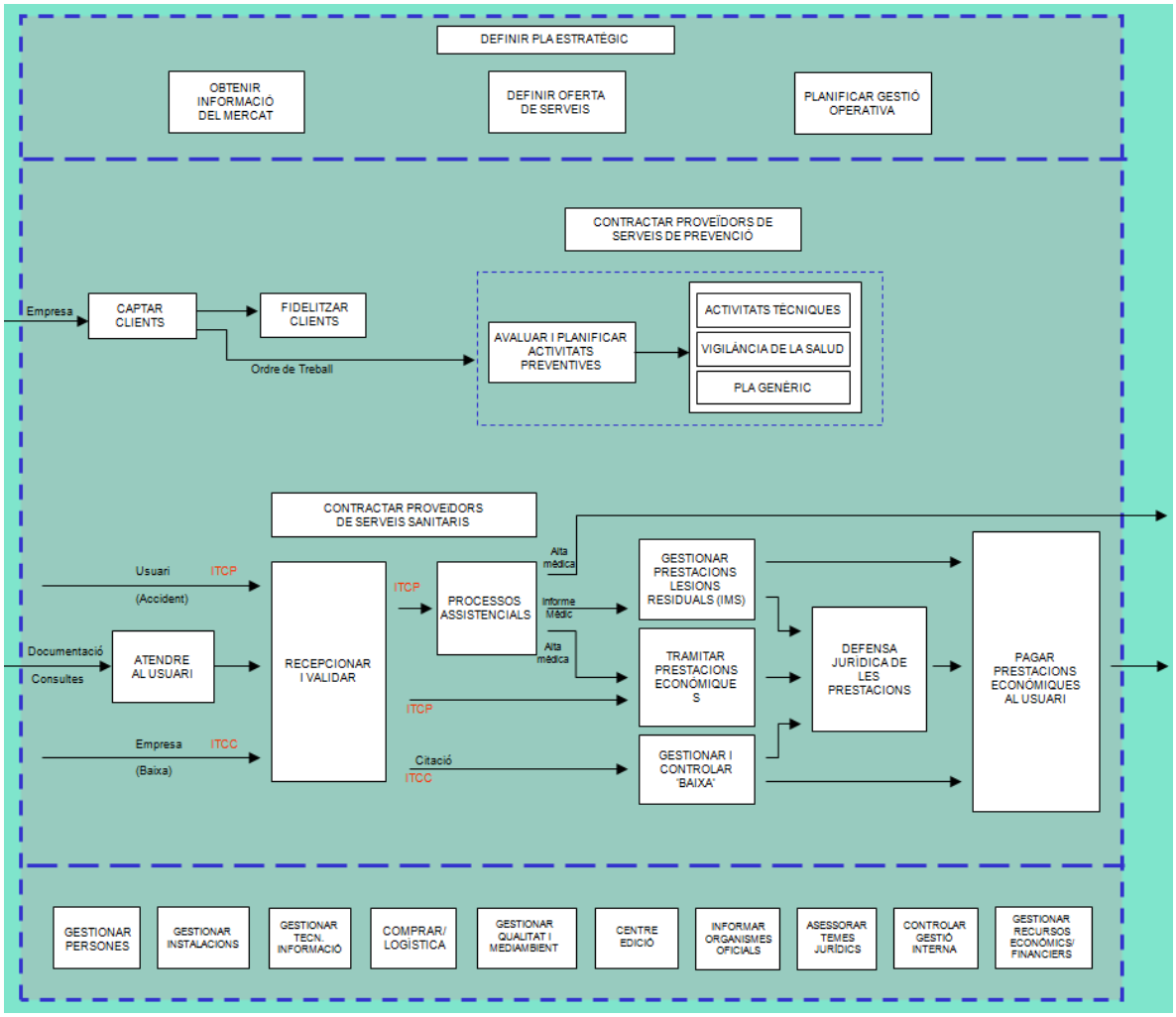
L'estratègia serà doncs que totes les normes convergeixin en aquesta mateixa estructura comú, amb el mateix contingut, idèntica redacció en els requisits normatius, excepte a l'apartat 8 "Operació" que serà en el que després d'un primer apartat també comú 8.1 de planificació i control operacional, cada norma desenvoluparà els seus requisits específics (de seguretat, de continuïtat, de gestió energètica... etc)

18.2. ANÀLISIS DELS PROCESSOS DE NEGOCI.

El nou enfoc de treball de la ISO 9001 Obliga a treballar per processos. Entenem com a procés l'activitat que transforma elements d'entrada en elements de sortida amb un valor afegit. Aquest enfoc ja el realitzava la ISO 14001. En la norma 27001, analitzem també el Risc dels actius i els classifiquem per processos de negoci. Així doncs entenem que el punt de partida de la implementació dels Sistemes de Gestió Integrats a la organització son els processos de negoci de la mateixa, així que per tal de poder-hi aplicar les normatives de SGI en primer lloc hem de tenir clar els processos de negoci. Almenys una visió general del mateix.

Per portar a terme aquesta pràctica crearem un possible mapa de processos de negoci alineat amb el pla estratègic de la Organització. De la Mútua Interuniversitària. On hi podem observar elements d'entrada i elements de sortida amb un servei o valor afegit.

MAPA DELS PROCESSOS DE NEGOCI



19. GLOSARI DE TERMES

- MISTIC: Master Universitari de Seguretat de les TIC
- CISA: Certified Information Systems Auditor. Certificat d'Auditor de Sistemes de la Informació.
- SGSI: Sistema de Gestió de Seguretat de la Informació.
- PDCA: Plan Do Chek Act. (Cicle de millora continua).
- SOA: Statement of Applicability, Document d'aplicabilidad.
- AMAT: Associació de Mútues d'Accidents de Treball.
- Risc Intrínsec: Es aquell que pateix un actiu davant d'una amenaça sense aplicar cap salvaguarda.
- Risc Efectiu: Es el que pateix un actiu davant d'una amenaça un cop aplicades les salvaguardes que li afecten.
- Risc Residual: És el risc que la Organització ha establert com a risc assumible per la mateixa i recolzat per la direcció.
- Salvaguarda: Aplicació de un % determinat per l'autor del Anàlisis de Riscos dels controls que afecten a un determinat objectiu amb el fi de protegir l'actiu.
- Vulnerabilitat: Una vulnerabilitat és una debilitat en els procediments de seguretat, disseny, implementació o control intern que podria ser explotada (accidentalment o intencionadament) i que resulta en una bretxa de seguretat o una violació de la política de seguretat de sistemes.
- Amenaça: Es tota circumstància, event o persona que te el potencial de causar dany a un sistema, en forma de robatori, destrucció, divulgació, modificació de dades o denegació de servei (DoS).
- Procés: activitat que transforma elements d'entrada en elements de sortida amb un valor afegit.
- CMM (Capacity Maturity Model). Model de Maduresa de capacitats. Es un model d'avaluació de Maduresa dels processos d'una Organització.

20. ANNEXOS

Tots els Annexos al present document es troben en una carpeta adjunta al mateix anomenada Annexos, des de el propi document s'han generat links o enllaços relatius a aquesta carpeta, Adjuntem una llista a continuació dels diferents Annexos que hi podem trobar i el link de direccionalment directe als mateixos. (Caldrà fer Ctrl+clic per accedir-hi).

Es desenvoluparà com a opció de millora un sistema documental mitjançant una aplicació específica per la SGSI.

Contingut	*Fitxer*
Annex A. Taula Excel amb SOA la Anàlisis diferencial	"Annex A.- SOA - Anàlisis diferencial TFM.xlsx"
Annex A2. Infraestructures i Equipaments.	"Annex A2.Infraestructures i Equipament.docx"
Annex B. d'estudi Comparatiu de les diferents normes	"Annex B-Comparativa Normes s.n"
Annex C. Quadre Resum Controls 27002:2013	"Annex C -Controls-ISO27002-2013.pdf"
Anàlisis i avaluació del Risc de Confidencialitat	"Annex D -Risc Confidencialidad.xls"
Anàlisis i avaluació del Risc de Risc Disponibilitat	"Annex E -Risc Disponibilitat.xls"
Anàlisis i avaluació del Risc de Risc d'Integritat	"Annex F -Risc integritat.xls"
Política de Seguretat de la Mutua Interuniversitària.	"Annex G. Política de Seguretat.docx"
Analisi Funcional de Gestió del Risc	"Annex H. Analisi Funcional Gestió del Risc"
Annex I. Projectes d'Alineació amb els Objectius del Pla Director	"Annex I. Projectes d'Alineacio´ amb els Objectius del Pla Director.docx"
Informe Final de l'Auditoria de Compliment de la ISO.27001/27002.	"Annex J.Auditoria de Compliment de la ISO"
Planificació Previa de l'Auditoria de Compliment.	"Annex K.Pla d'auditoria Interna"
Document de selecció de controls d'auditoria.	"Annex L.Selecció de Controls d'auditoria"
Segon document d'Analisis diferencial de maduresa, fruit de la implantació de controls, auditoria i projectes.	"Annex A3-SOA-Analisis diferencial TFM.V.2"
Revisió del Sistema per la direcció	"Annex M.Revisio´ del sistema per la direcció"
Presentació TFM. (Power Point)	"Presentació TFM"

21. REFERÈNCIES

Temàtica	Localització
ISO IEC 27001:2014	Enviada per Aenor PDF.
ISO IEC 27002:2015	PDF
SOA	Pepared by Richard O Regalado www.ISO27001security.com
FODA	http://www.calidad-gestion.com.ar/rec_gratuitos/articulos/analisis_foda.html
Integració Sistemes de Gestió.	https://calidadgestion.wordpress.com/2013/10/14/metodos-para-integrar-sistemas-de-gestion/
Integració dels sistemes de Gestió	http://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/
Magerit	2012_Magerit_v3_libro1_método_es_NIPO_630-12-171-8.pdf
Mètriques e Indicadors	815_Metricas_e_indicadores_en_el_ENS-feb14.pdf
Integració de SG	LA INTEGRACIÓN DE SISTEMAS DE GESTIÓN NORMALIZADOS SOBRE LA BASE DE LOS PROCESOS (Integracion-de-SG.pdf)
Gestió de Riscos	Norma ISO 31000 versión 2009: Gestió de Riesgos – Principios y Guías (Traducción libre)
Gestió de Riscos	ISO_iec_27005-2008
Comparativa Metodologies Anàlisis de Riscos	http://www.audea.com/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias/
OSHAS	Norma OHSAS 18001.pdf
Referències Històriques	http://www.amat.es/mutuas/historia.3php
Planells 3D	http://www.sweethome3d.com/es/download.jsp
Quadre 27002:2013	www.iso27001.es
Integració Sistemes de Gestió	https://www.icai.es/articulo-revista/integracion-de-sistemas-de-gestion-basados-en-normas/
Magerit	http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=ca#.WOUNSKLfOUk
Annex SL	http://www.apcergroup.com/espana/index.php/es/newsroom/769/anexo-sl-para-una-mejor-integracion-de-los-sistemas-de-gestion
Anexo SL	https://grliberato.wordpress.com/2015/05/13/iso-anexo-sl/
PAS 99	https://www.bsigroup.com/es-ES/PAS-99-Sistemas-de-Gestion-

	Integrados/
Annex SL (ii)	https://www.securityartwork.es/2013/09/05/sistemas-de-gestion-integrados-anexo-sl-ii/
Integrar diferents normes	http://www.aspectosprofesionales.info/2013/06/integrar-diferentes-normas-iso-gracias_20.html
OCSInventory	https://www.ocsinventory-ng.org/en/
Diferents Termes	https://www.wikipedia.org/ https://ca.wikipedia.org/wiki/Portada